Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Проєктування телекомунікаційної мережі в торговому центрі
(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІз-21-1*
Данило ЖДАНОВ
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц. Наталія ХАРЧЕНКО*
(посада, власне ім'я, прізвище)

Допускається до захисту
Завідувач кафедри _____ *Валерій БЕЗРУК*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / Данило Жданов /

Керівник / Наталія Харченко /

Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання
Кафедра *Інформаційно-мережної інженерії*
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Жданову Данилу Михайловичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Проєктування телекомунікаційної мережі в торговому центрі*

затверджена наказом університету від 02 травня 2025 р. № 63 Стз

2. Термін подання здобувачем роботи до екзаменаційної комісії 24 червня 2025 р.

3. Вихідні дані до роботи *Провести планування телекомунікаційної мережі торгового центру «Київ» м. Суми. Будинок має три поверхи, перший поверх містить торгові павільйони, другий – офісні приміщення, третій конференц-зал. Обрати технологію для передачі даних, розрахувати характеристики проєктованої мережі для визначення необхідної пропускної здатності, що впливає на подальший вибір обладнання. Визначити ієрархію мережі, місця розміщення мережного обладнання. Визначити методику керуванням трафіку у розробленій мережі.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Огляд базових технологій доступу у локальних мережах
2. Розрахунок пропускної спроможності проєктованої мережі
3. Вибір обладнання для проєктованої мережі
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета і актуальність кваліфікаційної роботи; стандарт Ethernet; класифікація бездротових технологій; досяжні швидкості стандарту 802.11ac; основи стандарту 802.1Q; логічна та фізична схема мережі торгового центру; організація VLAN у мережі; вибір обладнання; висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*02.05.25*	*виконано*
2	*Підбір літератури за темою роботи.*	*03.05-03.06.25*	*виконано*
3	*Огляд базових технологій доступу у локальних мережах*	*04.06-06.06.25*	*виконано*
4	*Розрахунок пропускної спроможності проєктованої мережі*	*07.06-13.06.25*	*виконано*
5	*Вибір обладнання для проєктованої мережі*	*14.06-20.06.25*	*виконано*
6	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*21.06-26.06.25*	*виконано*

Дата видачі завдання 02 травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Наталія Харченко
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 70 с., 18 рис., 15 табл., 10 джерел, 1 додаток.

Об'єкт дослідження – телекомунікаційна мережа торгового центру.

Мета роботи – провести планування телекомунікаційної мережі торгового центру.

Основною причиною створення локальної мережі є бажання надати користувачам швидкий доступ до корпоративних даних. Застосування мережі сприяє поліпшенню комунікацій, а саме до вдосконалення обміну інформацією та взаємодії між працівниками компанії, а також з її клієнтами та постачальниками.

У роботі було розглянуто найпоширеніші технології передачі даних, на основі яких буде відбуватися проєктування мережі. Визначено оптимальний варіант побудови – гібридна мережа з використанням технології Ethernet у дротовій частині мережі та технології Wi-Fi стандарту 802.11ac для надання доступу до Інтернет клієнтам торгового центру та співробітникам. Вибір обладнання ґрунтувався на таких критеріях: технічні параметри, можливості застосування, ціна та інші характеристики проектованої мережі. У розрахунковій частині роботи були проведені розрахунки корисного трафіку мережі та коефіцієнта її завантаження. Для поділу мережі на сегменти застосовувалася технологія 802.1Q VLAN.

ЛОКАЛЬНА МЕРЕЖА, ETHERNET, VLAN, 802.11AC, ACL.

THE ABSTRACT

Explanatory slip 70 p., 18 fig., 15 tab., 10 sources, 1 attach.

Object of research - telecommunications network of the shopping centre.

The purpose of the work - plan the telecommunications network of the shopping centre.

The main reason for creating a local area network is to provide users with quick access to corporate data. The use of a network helps to improve communications, namely, to improve the exchange of information and interaction between company employees, as well as with its customers and suppliers.

The paper considers the most common data transmission technologies that will be used to design the network. The best option was determined - a hybrid network using Ethernet technology in the wired part of the network and Wi-Fi 802.11ac technology to provide Internet access to the shopping centre's customers and employees. The choice of equipment was based on the following criteria: technical parameters, application possibilities, price and other characteristics of the projected network. In the calculation part of the work, we calculated the network's payload and load factor. The 802.1Q VLAN technology was used to divide the network into segments.

LOCAL AREA NETWORK, ETHERNET, VLAN, 802.11AC, ACL.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ACL – Access Control List – список контролю доступу;

CSMA/CD – Carrier Sense Multiple Access with Collision Detection – множинний доступ з контролем несучої і виявленням колізій;

DSSS – Direct Sequence Spectrum Spread – модуляція широкої смуги, зв'язок із розширеним спектром прямої послідовності;

IEEE – Institute of Electrical and Electronics Engineers – міжнародна організація інженерів у галузі електротехніки, радіоелектроніки та радіоелектронної промисловості;

MAC – Media Access Control – управління доступом до середовища;

MIMO – Multiple Input-Multiple Output – «множинний вхід - множинний вихід»;

MCS – Modulation and Coding Scheme – індекс модуляції та схеми кодування;

QoS – Quality of Service – якість надання послуг;

OFDM – Orthogonal Frequency Division Multiplexing – ортогональне частотне мультиплексування;

PoE – Power over Ethernet – стандарт живлення через кабель низько потужних пристроїв;

VLAN – Virtual Local Area Network – віртуальна локальна мережа;

UTP – Unshielded Twisted Pair – неекранована кручена пара;

ЛОМ – локальна обчислювальна мережа;

ПВХ – полівінілхрорид.

ВСТУП

Основною причиною створення локальної мережі є бажання надати користувачам швидкий доступ до корпоративних даних.

Застосування мережі сприяє поліпшенню комунікацій, а саме до вдосконалення обміну інформацією та взаємодії між працівниками компанії, а також з її клієнтами та постачальниками. Мережі зменшують потребу в інших способах передачі інформації, як-от телефон або звичайна пошта. Зазвичай комп'ютерні мережі впроваджуються в компаніях через можливість використання електронної пошти.

Звісно, комп'ютерні мережі стикаються з певними проблемами (труднощі зі сумісністю програмного забезпечення, виклики у передачі повідомлень через канали зв'язку з урахуванням забезпечення надійності та ефективності), проте основним підтвердженням їхньої ефективності є їх широке розповсюдження.

Мета кваліфікаційної роботи полягає у розробці телекомунікаційної мережі на території Торгового центру «Київ» м. Суми. Мережа охопить 3 поверхи. Для досягнення мети встановимо наступні завдання:

- ознайомитися з теоретичними аспектами технологій Ethernet та Wi-Fi;
- розрахувати характеристики проектованої мережі;
- підібрати найкраще обладнання для проекту;
- провести сегментування мережі шляхом с творення VLAN для покращення керування трафіком;
- визначити місця для інсталяції точок доступу.

1 ОГЛЯД БАЗОВИХ ТЕХНОЛОГІЙ ДОСТУПУ У ЛОКАЛЬНИХ МЕРЕЖАХ

1.1 Стандарт Ethernet

Ethernet - це технологія передачі даних, що базується на пакетах, яка зазвичай використовується в мережах локального обчислювального зв'язку. Стандарти Ethernet охоплюють використання кабельних з'єднань та електричних сигналів на фізичному шарі, а також визначають структуру кадрів і протоколи для контролю доступу до медіа на канальному шарі моделі OSI. Переважно, Ethernet регулюється стандартами IEEE серії 802.3. У середині 90-х років Ethernet став домінуючою технологією в області локальних обчислювальних мереж (ЛОМ), замінивши такі застарілі системи, як Arcnet, FDDI та Token Ring [1].

1.1.1 Історія створення

Ethernet технологію було створено в рамках численних ініціатив корпорації Xerox PARC. Поширена думка полягає в тому, що винахід Ethernet датується 22 травня 1973 року, коли Роберт Меткалф (Robert Metcalfe) представив звіт для керівництва PARC, висвітлюючи можливості технології Ethernet. Проте, офіційні права на технологію Меткалф здобув лише через декілька років. У 1976 році він разом зі своїм асистентом Девідом Боггсом (David Boggs) опублікували брошуру з назвою «Ethernet: Розподілене комутування пакетів для локальних комп'ютерних мереж». Меткалф залишив Xerox у 1979 році та заснував компанію 3Com з метою розвитку комп'ютерів та локальних обчислювальних мереж. Він зміг переконати DEC, Intel та Xerox об'єднати зусилля для розробки стандарту Ethernet (DIX). Цей стандарт був вперше опублікований 30 вересня 1980 року. Він започаткував конкуренцію з іншими великими запатентованими технологіями: Token Ring і ARCNET, які згодом були витіснені з ринку завдяки масовому виробництву продукції на базі Ethernet. У ході цієї конкуренції 3Com виросла в провідну компанію в цій сфері [1].

1.1.2 Технологія стандарту Ethernet

У початкових стандартах (Ethernet v1.0 та Ethernet v2.0) було зазначено використання коаксіального кабелю як передавального середовища, але згодом з'явилась можливість застосування крученої пари та оптоволокна [1].

Причини переходу на кручену пару включали:

- здатність працювати в дуплексному режимі;

- менша ціна кабелю «крученої пари»;

- підвищена надійність мереж при дефектах у кабелі;

- краща захищеність від перешкод при використанні диференційного сигналу;

- можливість живлення через кабель низько потужних пристроїв, таких як IP-телефони (стандарт Power over Ethernet, PoE);

- відсутність електричного з'єднання (проходження струму) між вузлами мережі. При використанні коаксіального кабелю в умовах України, де часто не заземлюють комп'ютери, використання коаксіального кабелю часто призводило до пробою мережевих карт, а іноді навіть до повного «вигоряння» системного блоку.

Потреба збільшення довжини сегмента без додаткових повторювачів стала причиною переходу на оптичний кабель.

Метод керування доступом (для мережі на коаксіальному кабелі) - множинний доступ з контролем несучої і виявленням колізій (CSMA/CD, Carrier Sense Multiple Access with Collision Detection). Цей метод передачі даних використовується лише в мережах, де всі пристрої підключені до спільного каналу зв'язку, як у випадку з логічною шиною або радіомережею. Кожен комп'ютер в такій мережі має прямий доступ до цього каналу і може використовувати його для обміну даними з будь-яким іншим комп'ютером (рис. 1.1). При цьому, всі пристрої в мережі можуть майже миттєво (з урахуванням часу, необхідного сигналу для поширення) отримувати інформацію, яку передає будь-який інший пристрій. Простота підключення є однією з ключових причин популярності Ethernet. Такий спільний канал зв'язку часто називають каналом колективного доступу.

Швидкість передачі даних 10 Мбіт/с, розмір пакета від 72 до 1526 байт. Кількість вузлів в одному сегменті мережі, що розділяється, обмежена граничним значенням в 1024 робочих станції (специфікації фізичного рівня

можуть встановлювати більш жорсткі обмеження, наприклад, до сегмента тонкого коаксіалу може підключатися не більше 30 робочих станцій, а до одного сегмента на базі товстого коаксіалу - не більше 100). Наявність граничного значення кількості вузлів, в основному спричинена напівдуплексним режимом роботи [1].

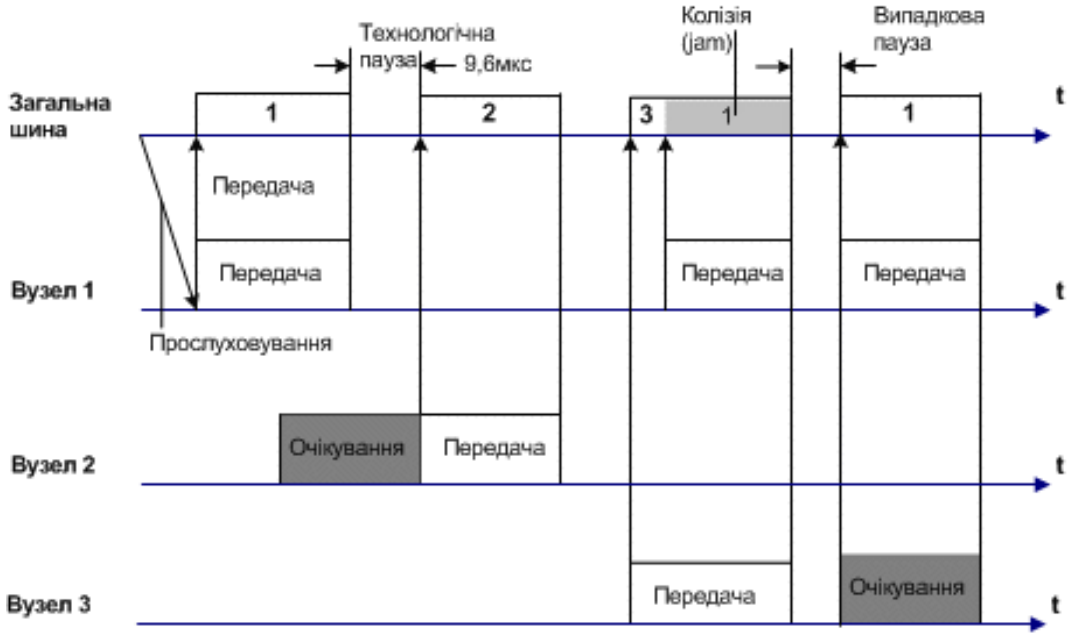

Рисунок 1.1 – Принцип роботи CSMA/CD

У 1995 році було прийнято стандарт IEEE 802.3u Fast Ethernet із швидкістю 100 Мбіт/с, що дозволило працювати в повнодуплексному режимі. У 1997 році з'явився стандарт IEEE 802.3z Gigabit Ethernet із швидкістю 1000 Мбіт/с для передачі через оптоволокно, а через два роки - для передачі по крученій парі [1].

1.1.3 Різновиди фізичних стандартів Ethernet

Залежно від швидкості передачі даних та середовища передачі, існують різноманітні технології передачі. Без врахування методу передачі, стек мережевих протоколів та програми функціонують однаково у більшості згаданих випадків. Велика кількість Ethernet-карт та інших пристроїв підтримують декілька рівнів швидкості передачі даних, застосовуючи автоматичне визначення (autonegotiation) швидкості та дуплексну передачу для забезпечення оптимального з'єднання між двома комп’ютерами. У випадку,

коли автоматичне визначення зазнає невдачі, швидкість налаштовується відповідно до характеристик партнера і активується режим напівдуплексної передачі. Наприклад, наявність у пристрою порту Ethernet 10/100 свідчить про можливість роботи з технологіями 10BASE-T та 100BASE-TX, тоді як порт Ethernet 10/100/1000 – забезпечує підтримку стандартів 10BASE-T, 100BASE-TX та 1000 BASE-TX [2].

10BASE-5, IEEE 802.3 (також відомий як "Товстий Ethernet") - це первісна версія технології зі швидкістю передачі даних 10 Мбіт/с. Відповідно до раннього стандарту IEEE, вона використовує коаксіальний кабель з хвильовим опором 50 Ом (RG-8) та максимальною довжиною сегмента у 500 метрів [2].

10BASE-2, IEEE 802.3a (відомий як "Тонкий Ethernet") - застосовує кабель RG-58 з максимальною довжиною сегмента у 185 метрів. Комп'ютери з'єднуються між собою, для підключення кабелю до мережевої карти потрібен Т-конектор, а на кабелі має бути BNC-конектор. Необхідно мати термінатори на обох кінцях кабелю. Цей стандарт був основною технологією Ethernet протягом багатьох років [2].

StarLAN 10 - Перша технологія, яка використовувала кручені пари для передачі даних зі швидкістю 10 Мбіт/с. Пізніше еволюціонувала у стандарт 10BASE-T. Хоча теоретично до одного кабелю (сегменту) крученої пари можна підключити більше двох пристроїв, що працюють у симплексному режимі, така схема ніколи не використовується в Ethernet, на відміну від роботи з коаксіальним кабелем, який побудований за топологією «шина». Термінатори для роботи з крученою парою інтегровані в кожен пристрій, тому застосування додаткових зовнішніх термінаторів не потрібно [2].

Класичний Ethernet

10BASE-T, IEEE 802.3i - використовує 4 дроти кабелю крученої пари (дві скручені пари) категорії 3 або категорії 5. Максимальна довжина сегмента становить 100 метрів [2].

FOIRL - (скорочення від англ. Fiber-optic inter-repeater link). Початковий стандарт для технології Ethernet, який передбачає використання оптичного кабелю. Максимальна відстань передачі без повторювача становить 1 км [2].

10BASE-F, IEEE 802.3j - загальна назва для групи стандартів Ethernet зі

швидкістю 10 Мбіт/с, які використовують оптичний кабель на відстань до 2 кілометрів: 10BASE-FL, 10BASE-FB та 10BASE-FP. Серед них лише 10BASE-FL отримав широке розповсюдження [2].

10BASE-FL (Fiber Link) - вдосконалена версія стандарту FOIRL. Вдосконалення полягає у збільшенні довжини сегмента до 2 км [2].

10BASE-FB (Fiber Backbone) – стандарт наразі не використовується, призначений для з'єднання повторювачів у магістралі [2].

10BASE-FP (Fiber Passive) – топологія "пасивна зірка", де повторювачі не потрібні - ніколи не використовувалася [2].

Швидкий Ethernet (Fast Ethernet, 100 Мбіт/с)

100BASE-T - універсальна назва для стандартів, які використовують виту пару як медіум для передачі даних. Максимальна довжина сегмента становить до 100 метрів. Охоплює стандарти 100BASE-TX, 100BASE-T4 та 100BASE-T2 (рис. 1.2) [2].

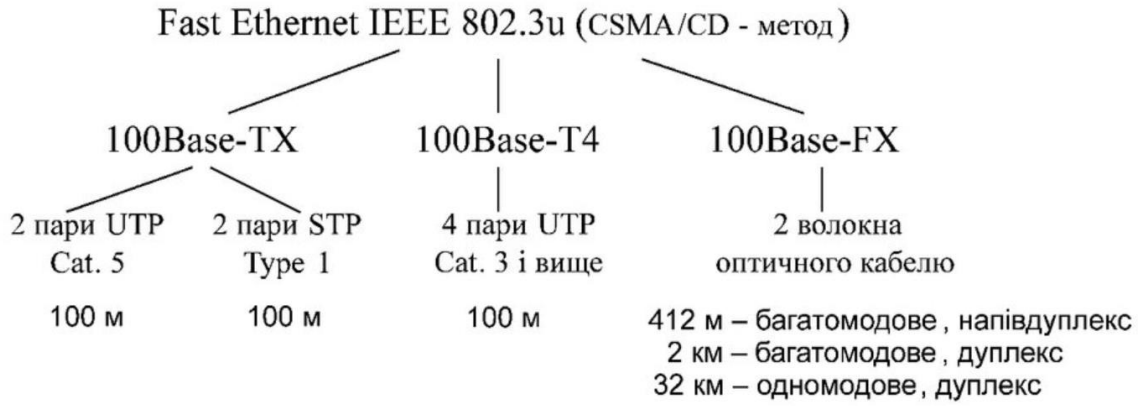

Рисунок 1.2 – Структура фізичних стандартів Fast Ethernet

100BASE-TX, IEEE 802.3u – еволюція стандарту 10BASE-T для застосування в мережах з топологією «зірка». Використовується вита пара категорії 5, де активні лише дві пари неекранованих проводів, підтримується двонаправлена передача даних, дистанція до 100 м [2].

100BASE-T4 - стандарт, який застосовує виту пару категорії 3. Використовуються усі чотири пари проводів, передача даних відбувається в напівдуплексному режимі. На практиці не застосовується [2].

100BASE-T2 - стандарт, який застосовує виту пару категорії 3.

Використовуються тільки дві пари проводів. Підтримується повний дуплекс, коли сигнали розповсюджуються в протилежних напрямках з кожної пари. Швидкість передачі в одному напрямку становить 50 Мбіт/с. На практиці не застосовується [2].

100BASE-SX - стандарт, який використовує багатомодове оптичне волокно. Максимальна довжина сегмента становить 400 метрів у напівдуплексному режимі (для надійного виявлення колізій) або 2 кілометри у повному дуплексі [2].

100BASE-FX – стандарт, який використовує одномодове оптичне волокно. Максимальна довжина обмежена тільки рівнем затухання в оптичному кабелі та потужністю передавачів, згідно з різними джерелами від 2 до 10 кілометрів [2].

100BASE-FX WDM – стандарт, який використовує одномодове оптичне волокно. Максимальна довжина обмежена тільки рівнем затухання у волоконно-оптичному кабелі та потужністю передавачів. Існують два типи інтерфейсів, які відрізняються довжиною хвилі передавача і позначаються числами (довжина хвилі) або однією латинською літерою A (1310) або B (1550). У парі можуть функціонувати тільки сумісні інтерфейси: з одного боку передавач на 1310 нм, з іншого - на 1550 нм [3].

Гігабітний Ethernet (Gigabit Ethernet, 1 Гбіт/с)

1000BASE-T, IEEE 802.3ab - це стандарт, який застосовує кручені пари категорії 5e. У процесі передачі даних використовуються 4 пари. Швидкість передачі складає 250 Мбіт/с на кожну пару. Застосований метод кодування - PAM5, при цьому основна гармоніка має частоту 625 МГц. Максимальна відстань становить до 100 метрів [3].

1000BASE-TX було розроблено Асоціацією Телекомунікаційної Промисловості (англ. Telecommunications Industry Association, TIA) і представлено у березні 2001 року як «Специфікація фізичного рівня для дуплексного Ethernet на 1000 Мбіт/с (1000BASE-TX) для симетричних кабелів (ANSI/TIA/EIA-854-2001)» (англ. «A Full Duplex Ethernet Specification for 1000 Mbis/s (1000BASE-TX) Operating Over Category 6 Balanced Twisted-Pair Cabling (ANSI/TIA/EIA-854-2001)». У кожному напрямку), що значно спрощує дизайн приймально-передавальних пристроїв. У якості кабелю, для 1000BASE-TX

допускається використання лише кабелю 6 категорії [2].

1000BASE-X - це узагальнена назва для стандартів з використанням змінних приймачів GBIC або SFP [2].

1000BASE-SX, IEEE 802.3z - стандарт, який використовує багатомодове оптичне волокно. Максимальна дистанція передачі сигналу без використання повторювачів досягає 550 метрів [2].

1000BASE-LX, IEEE 802.3z – стандарт, який застосовує одномодове оптичне волокно. Максимальна дистанція передачі сигналу без використання повторювачів становить до 5 км [2].

1000BASE-CX – це стандарт для коротких дистанцій (до 25 метрів), який використовує твінаксіальний кабель з хвильовим опором 75 Ом (для кожного з двох провідників). Замінений стандартом 1000BASE-T і наразі не застосовується [2].

1000BASE-CX – стандарт для коротких дистанцій (до 25 метрів), який використовує твінаксіальний кабель з хвильовим опором 75 Ом (для кожного з двох провідників). Замінений стандартом 1000BASE-T і наразі не застосовується [2].

1000BASE-LH (Long Haul) – стандарт, який використовує одномодове оптичне волокно. Максимальна дистанція передачі сигналу без повторювача досягає 100 км [2].

10-гігабітний Ethernet

Нова версія стандарту Ethernet на 10 гігабіт охоплює сім фізичних стандартів для мереж LAN, MAN та WAN. Наразі вона детально викладена в поправці IEEE 802.3ae і має бути інтегрована в майбутню ревізію стандарту IEEE 802.3 [3].

10GBASE-CX4 - це технологія Ethernet на 10 гігабіт для коротких дистанцій (до 15 метрів), яка використовує мідний кабель CX4 та конектори InfiniBand [3].

10GBASE-SR - це технологія Ethernet на 10 гігабіт для коротких дистанцій (до 26 або 82 метрів, залежно від типу кабелю), яка використовує багатомодове волокно. Вона також дозволяє здійснювати передачу на відстань до 300 метрів за допомогою нового багатомодового волокна (2000 МГц/км) [3].

10GBASE-LX4 – застосовує техніку ущільнення хвиль для підтримки

дистанцій від 240 до 300 метрів через багатомодове волокно. Також можлива передача на відстань до 10 кілометрів за допомогою одномодового волокна [3].

10GBASE-LR та 10GBASE-ER – ці стандарти дозволяють здійснювати передачу на відстані до 10 та 40 кілометрів відповідно [3].

10GBASE-SW, 10GBASE-LW та 10GBASE-EW – ці стандарти використовують фізичний інтерфейс, який є сумісним за швидкістю та форматом даних з інтерфейсом OC-192/STM-64 SONET/SDH. Вони аналогічні до стандартів 10GBASE-SR, 10GBASE-LR і 10GBASE-ER, оскільки використовують аналогічні типи кабелів і дистанції передачі [3].

10GBASE-T, IEEE 802.3an-2006 – затверджений у червні 2006 року після чотирьох років розробки. Використовує екрановану кручену пару. Дальність передачі – до 100 метрів [3].

1.2 Група стандартів Wi-Fi IEEE 802.11

На сьогоднішній день набувають популярності бездротові локальні мережі (WLAN). Вони переважно використовуються для забезпечення доступу до інформаційних ресурсів всередині приміщень. Наступною важливою областю застосування є створення публічних комерційних точок доступу, так званих хот-спотів (hotspots), у місцях з великим скупченням людей – таких як готелі, аеропорти, кафе, а також для створення тимчасових мереж під час проведення різноманітних заходів (виставок, семінарів) [4].

Для створення бездротових локальних мереж використовують стандарти сімейства IEEE 802.11 (рис. 1.3). Ці мережі також відомі під назвою Wi-Fi (Wireless Fidelity), і хоча назва Wi-Fi не зазначена безпосередньо у стандарті, бренд Wi-Fi став дуже популярним у всьому світі [4].

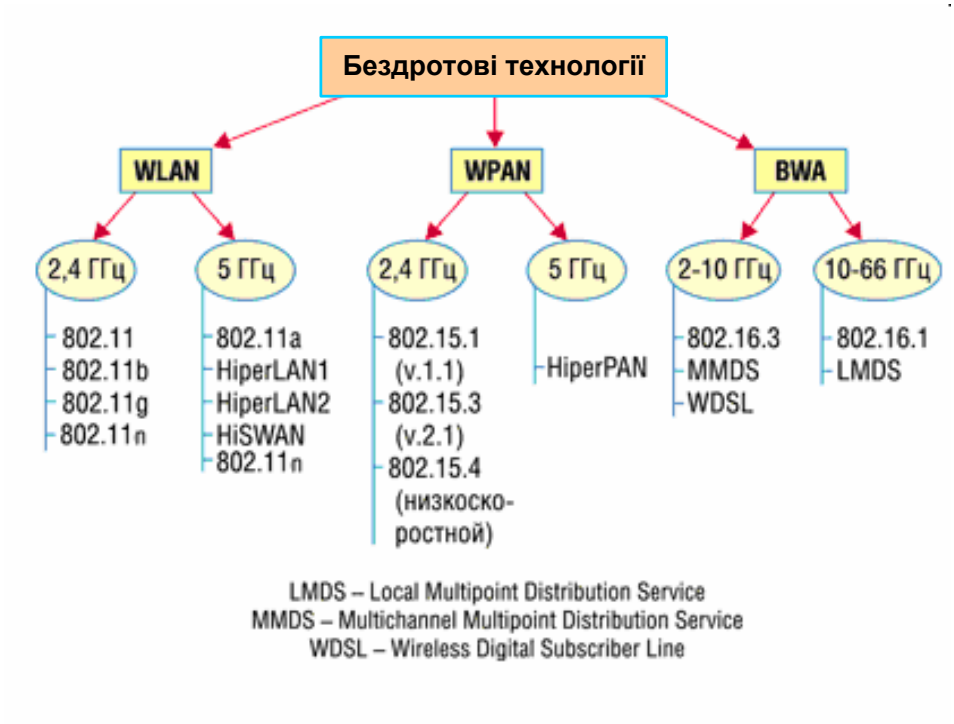

Рисунок 1.3 – Класифікація бездротових технологій

Організація IEEE (Institute of Electrical and Electronic Engineers) відповідає за розробку стандартів Wi-Fi 802.11 [4].

Основний стандарт для мереж Wi-Fi, IEEE 802.11, встановлює протоколи для найменших можливих швидкостей передачі даних.

IEEE 802.11b розширює можливості передачі даних, вносячи додаткові технічні обмеження. WECA (Wireless Ethernet Compatibility Alliance) активно популяризувала цей стандарт, який спочатку був відомий як Wi-Fi. Для роботи використовуються частотні канали в діапазоні 2.4GHz [4].

Стандарт був затверджений у 1999 році.

Застосована технологія радіочастот: DSSS.

Методи кодування: Barker 11 та CCK.

Типи модуляції: DBPSK та DQPSK,

Максимальна швидкість передачі даних у каналі становить: 1, 2, 5.5, 11 Mbps,

IEEE 802.11a пропонує значно вищі швидкості передачі даних порівняно з 802.11b. Використовуються частотні канали в діапазоні 5GHz. Протокол не сумісний з 802.11b [4].

Затверджено у 1999 році.

Технологія радіочастот, що використовується: OFDM.

Система кодування: Convoltion Coding.

Методи модуляції: BPSK, QPSK, 16-QAM, 64-QAM.

Максимальні швидкості передачі в каналі досягають: 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

IEEE 802.11g пропонує швидкості передачі даних, що еквівалентні 802.11a. Частотні канали розташовані в діапазоні 2.4GHz. Протокол сумісний з 802.11b [4].

Ратифіковано у 2003 році.

Застосовані технології радіочастот: DSSS та OFDM.

Методи кодування: Barker 11 та CCK.

Типи модуляції: DBPSK та DQPSK,

Максимальні швидкості передачі даних у каналі: 1, 2, 5.5, 11 Mbps на DSSS та 6, 9, 12, 18, 24, 36, 48, 54 Mbps на OFDM.

IEEE 802.11n – це найсучасніший комерційний стандарт Wi-Fi. У 802.11n використовуються частотні канали в діапазонах 2.4GHz та 5GHz. Сумісний з 11b/11a/11g. Проте рекомендується створювати мережі з використанням лише 802.11n, оскільки потрібно налаштувати спеціальні захисні режими для забезпечення зворотної сумісності зі старими стандартами, що може призвести до значного збільшення обсягу сигнальної інформації та зниження ефективності радіоінтерфейсу. Навіть один клієнт Wi-Fi 802.11g або 802.11b вимагатиме спеціального налаштування всієї мережі та миттєво знизить її загальну продуктивність [4].

Стандарт Wi-Fi 802.11n був опублікований 11 вересня 2009 року.

Підтримуються частотні канали Wi-Fi шириною 20MHz та 40MHz (2x20MHz).

Технологія радіочастот, що використовується: OFDM.

Застосовується технологія OFDM MIMO (Multiple Input Multiple Output) до рівня 4x4 (4 передавачі та 4 приймачі), з мінімумом 2 передавачів на точку доступу і 1 передавач на пристрій.

Для ефективної роботи мереж 802.11n точки доступу та клієнтські пристрої повинні узгоджувати кількість використовуваних просторових потоків та ширину каналу. Кількість просторових потоків залежить від кількості антен. Максимальна теоретична швидкість передачі даних стандарту 802.11n, що становить 600 Мбіт/с, досягається лише за умови використання чотирьох антен

для передачі та чотирьох для прийому (конфігурація 4x4).

Стандарт 802.11n використовує індекс модуляції та схеми кодування, що позначаються абревіатурою MCS (Modulation and Coding Scheme). MCS - це число, яке присвоюється кожній комбінації параметрів модуляції (всього їх 77). Кожна комбінація MCS визначає тип модуляції радіосигналу, швидкість кодування, тривалість захисного інтервалу та, як наслідок, швидкість передачі даних. Всі ці фактори разом визначають фактичну фізичну (PHY) швидкість передачі даних, яка може варіюватися від 6,5 Мбіт/с до 600 Мбіт/с, якщо використовуються всі можливості стандарту 802.11n. Приклади можливих MCS (Modulation & Coding Scheme) для 802.11n та максимальні теоретичні швидкості передачі даних у радіоканалі представлені в табл. 1.1.

Таблиця 1.1 – Індекс модуляції і схеми кодування (MCS) для 802.11n

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1 / 2	1	6.50	7.20	13.50	15.00
1	QPSK	1 / 2	1	13.00	14.40	27.00	30.00
2	QPSK	3 / 4	1	19.50	21.70	40.50	45.00
3	16-QAM	1 / 2	1	26.00	28.90	54.00	60.00
4	16-QAM	3 / 4	1	39.00	43.30	81.00	90.00
5	64-QAM	2 / 3	1	52.00	57.80	108.00	120.00
6	64-QAM	3 / 4	1	58.50	65.00	121.50	135.00
7	64-QAM	5 / 6	1	65.00	72.20	135.00	150.00
8	BPSK	1 / 2	2	13.00	14.40	27.00	30.00
9	QPSK	1 / 2	2	26.00	28.90	54.00	60.00
10	QPSK	3 / 4	2	39.00	43.30	81.00	90.00
11	16-QAM	1 / 2	2	52.00	57.80	108.00	120.00
12	16-QAM	3 / 4	2	78.00	86.70	162.00	180.00
13	64-QAM	2 / 3	2	104.00	115.60	216.00	240.00
14	64-QAM	3 / 4	2	117.00	130.00	243.00	270.00
15	64-QAM	5 / 6	2	130.00	144.40	270.00	300.00
16	BPSK	1 / 2	3	19.50	21.70	40.50	45.00
...	...	...	...	...	...	...	...
31	64-QAM	5 / 6	4	260.00	288.90	540.00	600.00

Тут SGI представляє собою інтервали захисту між фреймами. Кількість просторових потоків визначається як Spatial Streams. Type вказує на метод модуляції. Data Rate позначає максимальну теоретичну швидкість передачі даних у радіоканалі, виміряну в Мбіт/сек.

Необхідно зазначити, що наведені швидкості кореспондують з поняттям

channel rate і представляють максимально можливе значення за умов використання відповідного набору технологій у межах описуваного стандарту. Проте в реальних умовах досягнення цих значень неможливе через особливості технології стандарту Wi-Fi 802.11. Наприклад, значно впливає "політкоректність" у частині забезпечення CSMA/CA (пристрої WiFi постійно моніторять ефір і не можуть передавати дані, якщо канал зайнятий), необхідність підтвердження кожного юнікастового фрейму, напівдуплексний характер усіх стандартів Wi-Fi і лише 802.11ac/Wave-2 починає обходити це за допомогою MU. Ефективність стандартів 802.11 b/g/a ніколи не перевищує 50% в ідеальних умовах (наприклад, для 802.11g максимальна швидкість на користувача зазвичай не перевищує 22Мб/с), а для 802.11n ефективність може досягати до 60%. У випадку, коли мережа функціонує в захищеному режимі, що часто трапляється через змішане використання різних Wi-Fi-чіпів на різних пристроях у мережі, навіть вказана відносна ефективність може знизитися в 2-3 рази. Це стосується, зокрема, комбінації Wi-Fi пристроїв з чіпами 802.11b, 802.11g у мережі з точками доступу Wi-Fi 802.11g або Wi-Fi 802.11g/802.11b у мережі з точками доступу Wi-Fi 802.11n і т.д. [4].

Окрім основних стандартів Wi-Fi 802.11a, b, g, n, також використовуються додаткові стандарти для забезпечення різноманітних сервісних функцій [4]:

- 802.11d: Призначений для адаптації Wi-Fi-пристроїв до специфічних умов різних країн;

- 802.11e. Визначає класи якості QoS для передачі різноманітних медіафайлів і загалом медіаконтенту. Адаптація MAC-рівня для 802.11e встановлює якість, наприклад, для одночасної передачі аудіо та відео;

- 802.11f. Спрямований на стандартизацію параметрів точок доступу Wi-Fi різних виробників. Стандарт дозволяє користувачам безперебійно працювати з різними мережами під час переміщення між зонами покриття різних мереж;

- 802.11h. Використовується для уникнення конфліктів з метеорологічними та військовими радарами шляхом динамічного зменшення потужності випромінювання Wi-Fi обладнання або динамічної зміни частотного каналу при виявленні тригерного сигналу (у більшості країн Європи станції моніторингу за метеорологічними супутниками та супутниками зв'язку, а також радари військового призначення). Цей стандарт є обов'язковою

вимогою ETSI для обладнання, що допускається до експлуатації на території країн Європейського Союзу;

- 802.11i. У початкових версіях стандартів Wi-Fi 802.11 для забезпечення безпеки мереж Wi-Fi застосовувався алгоритм WEP. Вважалося, що цей метод здатен забезпечити конфіденційність та захист даних, переданих авторизованими користувачами бездротової мережі, від несанкціонованого доступу. Однак сьогодні цей захист можна обійти всього за кілька хвилин. Таким чином, у стандарті 802.11i були розроблені новітні методи захисту мереж Wi-Fi, які працюють на фізичному та програмному рівнях. Для забезпечення безпеки в мережах Wi-Fi 802.11 рекомендовано використовувати алгоритми Wi-Fi Protected Access (WPA), які також забезпечують сумісність між бездротовими пристроями різних стандартів та модифікацій. Протоколи WPA застосовують удосконалену версію шифрування RC4 та метод обов'язкової аутентифікації за допомогою EAP. Надійність та безпека сучасних мереж Wi-Fi залежить від протоколів перевірки конфіденційності та шифрування даних (RSNA, TKIP, CCMP, AES). Найкращим варіантом є використання WPA2 з шифруванням AES (і не забувайте про 802.1x з використанням механізмів тунелювання, як-от EAP-TLS, TTLS та інші);

- 802.11k. Цей стандарт спрямований на реалізацію балансування навантаження у радіопідсистемі мережі Wi-Fi. Зазвичай, у бездротовій локальній мережі абонентський пристрій підключається до точки доступу з найсильнішим сигналом. Часто це веде до перевантаження мережі в певній точці, коли до однієї точки доступу одночасно підключається багато користувачів. Для управління такими ситуаціями у стандарті 802.11k введено механізм, що обмежує кількість абонентів, які можуть підключитися до однієї точки доступу, і дозволяє створювати умови для підключення нових користувачів до іншої ТД, навіть якщо сигнал від неї слабкіший. Такий підхід збільшує загальну пропускну спроможність мережі за рахунок більш ефективного використання ресурсів;

- 802.11m. Усі поправки та виправлення до групи стандартів 802.11 зібрані у єдиному документі під назвою 802.11m. Перше видання 802.11m з'явилося у 2007 році, потім у 2011 році і так далі;

- 802.11p. Встановлює правила взаємодії Wi-Fi-обладнання, що переміщується зі швидкістю до 200 км/год повз стаціонарні точки доступу Wi-

Fi, розташовані на відстані до 1 км. Частина стандарту Wireless Access in Vehicular Environment (WAVE). Стандарти WAVE визначають архітектуру та додатковий набір сервісних функцій та інтерфейсів, які дозволяють забезпечити безпечний радіозв'язок між рухомими транспортними засобами. Ці стандарти розроблені для застосувань, таких як управління дорожнім рухом, моніторинг безпеки дорожнього руху, автоматизований збір платежів, навігація та маршрутизація транспорту та інше;

- 802.11r. Визначає процес швидкого автоматичного перемикання Wi-Fi-пристроїв при переході з зони покриття однієї точки доступу WiFi до іншої. Цей стандарт спрямований на підтримку мобільності, особливо важливий для мобільних/переносних пристроїв з Wi-Fi, таких як смартфони, планшети, Wi-Fi IP-телефони тощо. До введення цього стандарту, при переміщенні користувач часто втрачав зв'язок з однією точкою доступу і мусив шукати іншу, що займало багато часу. Існували приватні рішення для роумінгу (перемикання) між точками доступу, наприклад, CCKM від Cisco. Пристрої, що підтримують 802.11r, можуть заздалегідь реєструватися у сусідніх точках доступу та автоматично перепідключатися. Це значно скорочує час, протягом якого абонент залишається недоступним у мережах Wi-Fi;

- 802.11c. Цей стандарт розроблено для створення повноцінних мереж (Wireless Mesh), у яких кожен пристрій може виконувати роль як маршрутизатора, так і точки доступу. У випадку, коли найближча точка доступу є перевантаженою, трафік перенаправляється до найближчого вільного вузла. Таким чином, пакет даних переміщується від одного вузла до іншого, доки не досягне свого кінцевого пункту призначення. У цьому стандарті представлено нові протоколи на рівнях MAC і PHY, що дозволяють здійснювати широкомовну і мультикастову передачу, а також унікастову доставку через систему самоконфігуруючихся точок доступу Wi-Fi. Для цих цілей у стандарті використовується чотириадресний формат кадру;

- 802.11t. Цей стандарт був розроблений для стандартизації процесу тестування рішень на основі IEEE 802.11. Він описує методології тестування, методи вимірювань та обробки результатів, а також вимоги до тестового обладнання;

- 802.11u. Встановлює процедури для взаємодії мереж Wi-Fi з зовнішніми мережами. Стандарт має визначати протоколи доступу, пріоритетності та

обмеження для роботи з зовнішніми мережами. Наразі цей стандарт спричинив значний розвиток як у сфері розробки рішень – Hotspot 2.0, так і в організації міжмережевого роумінгу – з'явилася та розширюється група зацікавлених операторів, які разом працюють над питаннями роумінгу для своїх Wi-Fi мереж у рамках діалогу (Альянс WBA);

- 802.11v. У цьому стандарті розроблено зміни, спрямовані на поліпшення систем управління мережами на основі IEEE 802.11. Оновлення на рівнях MAC та PHY мають дозволити централізувати та систематизувати конфігурацію клієнтських пристроїв, що підключені до мережі;

- 802.11y. Додатковий стандарт для зв'язку у частотному діапазоні 3,65-3,70 ГГц. Розроблений для пристроїв нового покоління, які працюють з зовнішніми антенами на швидкостях до 54 Мбіт/с на відстані до 5 км у відкритому просторі. Стандарт ще не був завершений повністю;

- 802.11w. Встановлює методики та процедури для підвищення рівня захисту та безпеки управління доступом до мережі передачі даних (MAC). Стандарт організовує систему контролю за цілісністю даних, автентичністю їх джерела, запобіганням неавторизованому відтворенню та копіюванню, забезпеченням конфіденційності даних та іншими заходами захисту. У стандарті впроваджено захист управлінських кадрів (MFP: Management Frame Protection), а додаткові заходи безпеки допомагають протистояти зовнішнім атакам, таким як DoS. Більше про MFP можна дізнатися тут: 1, 2. Крім того, ці заходи забезпечують захист для найбільш вразливих мережевих даних, які передаються через мережі з підтримкою IEEE 802.11r, k, y [4].

Основні особливості технології 802.11ac

Технологія 802.11ac пропонує ряд переваг, що сприяють її швидкому прийняттю в нашому регіоні, подібно до того, як це відбувається у всьому світі. Основні переваги технології включають:

- значно вищу швидкість передачі даних (у порівнянні з Wi-Fi стандартом 802.11n);

- розширену зону покриття (у порівнянні з 11n);

- збільшення тривалості роботи батареї мобільних пристроїв (у 2-4 рази порівняно з 11n) [5].

Ключовими перевагами стандарту Wi-Fi 802.11ac є високі швидкості

передачі даних у радіоканалі та, відповідно, збільшена агрегована пропускна здатність точки доступу, а також удосконалені механізми управління активним та пасивним станами клієнтських пристроїв. Це призводить до значного збільшення часу роботи батареї мобільного пристрою.

Рішення на основі стандарту 802.11ac досягають високих швидкостей передачі даних завдяки тривимірній функціональній матриці:

1) збільшення кількості об'єднаних частотних каналів до: 80MHz або навіть 160MHz (порівняно з максимумом 40 MHz для 802.11n);

2) підвищена доступна модуляція: до QAM256 (максимум QAM64 для 802.11n);

3) вищий рівень MIMO: до 8 просторових потоків (для 802.11n до 4 потоків) [5].

Технологія 802.11ac функціонує лише на частотах Wi-Fi 5GHz. Таким чином, двосмугові точки доступу зазвичай продовжують використовувати 802.11n на частотах 2.4GHz.

Перше покоління пристроїв стандарту Wi-Fi 802.11ac (Wave-1) залишається напівдуплексною радіотехнологією. Ці пристрої зазвичай використовують частотні канали шириною до 80MHz і до трьох просторових потоків. Таким чином, можна виділити низький рівень продуктів 802.11ac зі швидкостями радіоканалу до 433Мб/с, середній рівень зі швидкостями до 867Мб/с і високий рівень зі швидкостями до 1,3Гб/с. Реальні швидкості передачі даних для користувачів будуть значно нижчими через проблеми з ефективністю у групі стандартів 802.11 (табл. 1.2). Зазвичай, реально доступний максимум не перевищує 60%. Точки доступу та Wi-Fi-маршрутизатори 802.11ac першої хвилі вже широко доступні у світі [5].

Друге покоління продуктів стандарту 802.11ac ще не доступне. Очікується, що друга хвиля 11ac спочатку підтримуватиме частотні канали до 160MHz, до чотирьох просторових потоків і технологію одночасної комунікації з кількома користувачами MU-MIMO (Multi User MIMO). MU-MIMO дозволяє одночасно відправляти декілька кадрів до різних користувачів у тому ж частотному спектрі. Таким чином, використовуючи кілька антен і відповідну технологію, точка доступу Wi-Fi може функціонувати як бездротовий комутатор. Однак, технологія обмежена максимальною кількістю доступних просторових потоків. Таким чином, якщо на точці доступу підтримуються три

просторових потоки і всі клієнти мають трипотокові пристрої (наприклад, MacBook Pro), то з точкою завжди взаємодіятиме лише один клієнт, навіть при підтримці MU-MIMO. Тому MU-MIMO особливо вигідно для мереж, де переважають мобільні пристрої, такі як смартфони та планшети, які мають максимум 2 просторові потоки, але зазвичай один. У випадку смартфонів з одним потоком і точки доступу Wi-Fi з трьома потоками і MU-MIMO, ми матимемо можливість роботи один до трьох, і точка зможе підтримувати до трьох клієнтів одночасно і паралельно [5].

Таблиця 1.2 - 802.11ac досяжні швидкості

Channel bandwidth	Transmit - Receive antennas	Modulation and coding etc	Typical client scenario	Throughput (individual link rate)	Throughput (aggregate link rate)
80 MHz	1x1	256-QAM 5/6, short guard interval	Smartphone	433 Mbps	433 Mbps
80 MHz	2x2	256-QAM 5/6, short guard interval	Tablet, PC	867 Mbps	867 Mbps
160 MHz	1x1	256-QAM 5/6, short guard interval	Smartphone	867 Mbps	867 Mbps
160 MHz	2x2	256-QAM 5/6, short guard interval	Tablet, PC	1.73 Gbps	1.73 Gbps
160 MHz	4x Tx AP, 4 clients of 1x Rx	256-QAM 5/6, short guard interval	Multiple smartphones	867 Mbps per client	3.47 Gbps
160 MHz	8x Tx AP, 4 clients with total of 8x Rx	256-QAM 5/6 , short guard interval	Digital TV, set-top box, tablet, PC, smartphone	867 Mbps to two 1x clients 1.73 Gbps to one 2x client 3.47 Gbps to one 4x client	6.93 Gbps
160 MHz	8x Tx AP, 4 clients of 2x Rx	256-QAM 5/6, short guard interval	Multiple set-top boxes, PCs	1.73 Gbps to each client	6.93 Gbps

Останні два варіанти із вісьмома просторовими потоками на даному етапі розвитку технології виглядають малоймовірними для масового виробництва та застосування [5].

1.3 Основи стандарту 802.1Q

IEEE 802.1Q представляє собою відкритий стандарт, що детально описує метод тегування трафіку для передачі даних про приналежність до VLAN. Через те, що 802.1Q не вносить зміни до заголовків кадрів, пристрої мережі, які не підтримують цей стандарт, здатні передавати трафік, не враховуючи його

VLAN приналежність [6].

802.1Q вставляє у кадр тег, що містить дані про приналежність трафіку до VLAN. Тег має розмір 4 байти і складається з наступних полів (рис. 1.4):

- Tag Protocol Identifier (TPID, ідентифікатор протоколу тегування). Довжина поля – 16 біт. Позначає, який протокол застосовується для тегування. Для 802.1Q використовується код 0x8100;

- Priority (Пріоритет). Довжина поля – 3 біти. Застосовується за стандартом IEEE 802.1p для встановлення пріоритету передаваного трафіку;

- Canonical Format Indicator (CFI, індикатор канонічного формату). Довжина поля – 1 біт. Визначає формат MAC-адрес. 0 означає канонічний формат, 1 - неканонічний. CFI застосовується для забезпечення сумісності між мережами Ethernet та Token Ring;

- Identifier VLAN (VID, ідентифікатор VLAN). Довжина поля – 12 біт. Вказує на приналежність кадру до певного VLAN. Можливі значення варіюються від 0 до 40.95 [6].

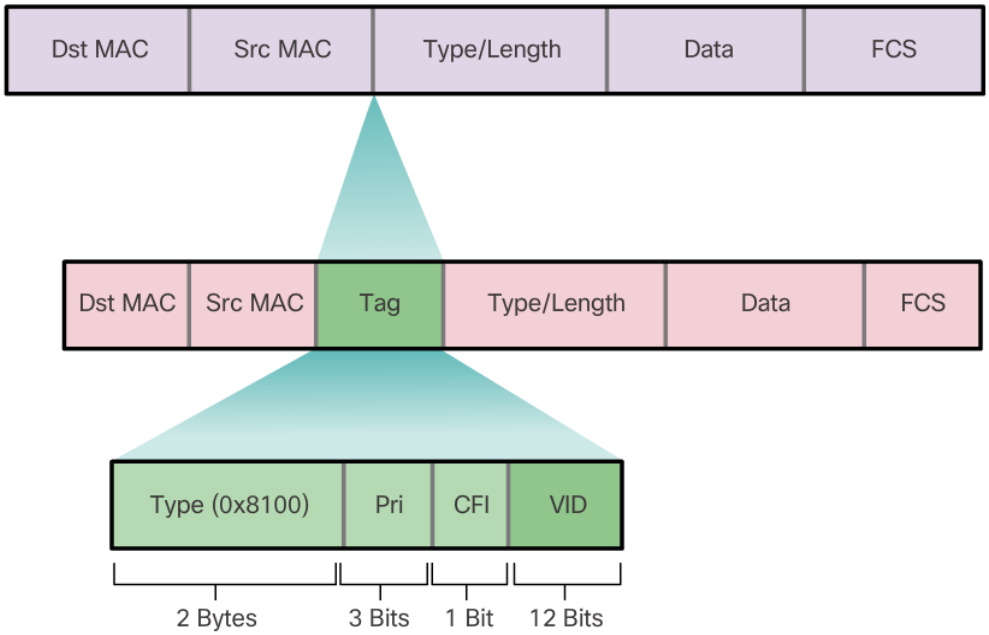

Рисунок 1.4 - Вставка тега 802.1Q в кадр Ethernet-II

При застосуванні стандарту Ethernet II, 802.1Q вставляє тег перед полем «Тип протоколу». Через зміну кадру, контрольна сума перераховується [6].

У рамках стандарту 802.1Q існує концепція Native VLAN, яка за замовчуванням є VLAN 1. Трафік, що проходить через цей VLAN, не підлягає

тегуванню.

Shortest Path Bridging Включено до IEEE 802.1Q-2014 [1].

Існує пропрієтарний протокол, аналогічний 802.1Q, розроблений компанією Cisco Systems ISL.

1.4 Типи кабелів

1.4.1 Вита пара

Вита пара може мати екранування або бути без нього.

Вона складається з однієї чи кількох пар провідників, що скручені між собою для підвищення якості прийому та відправлення сигналів (рис. 1.5). Провідники у складі пар виготовлені з цільного мідного дроту діаметром 0,4-0,6 мм. Скручування допомагає зменшити вплив зовнішніх та внутрішніх перешкод на передавані кабелем корисні сигнали, оскільки електромагнітні перешкоди впливають однаково на обидва проводи в парі [7].

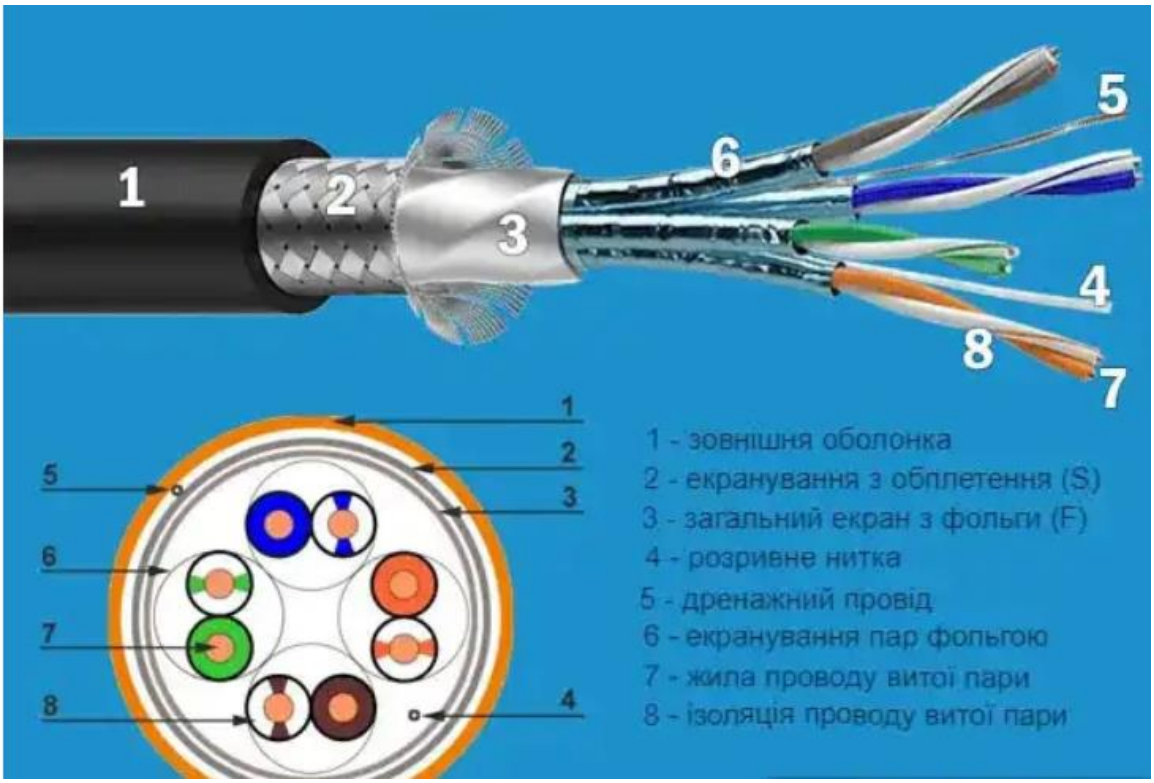

Рисунок 1.5 – Структура витої пари

У складі кабелю також знаходиться так звана «нитка для розрізу» (зазвичай виготовлена з капрону), яка слугує для полегшення доступу до

внутрішніх компонентів при зніманні зовнішньої оболонки. Коли її витягують, вона формує на оболонці поздовжній розріз, що дозволяє без зусиль дістатися до ядра кабелю без небезпеки ушкодження ізоляції проводів. Більше того, завдяки великій міцності на розтяг, нитка для розрізу відіграє захисну функцію [7].

Кожен провід захищено ізоляцією з ПВХ або поліпропілену. Зовнішня оболонка також зроблена з ПВХ. Для збільшення захисту від вологи кабель може бути оснащений оболонкою з поліпропілену. Залежно від виду кабелю можливі різні варіанти захисту:

- UTP або незахищена без загального екрану для пар проводів;

- FTP або фольгована, з екраном з алюмінієвої фольги;

- STP або захищена, із загальним екраном з мідної сітки, до того ж кожна кручена пара оточена окремим екраном;

- S/FTP або фольгована, екранована із загальним екраном із фольги, до того ж кожна пара додатково включена в екран [7].

Окрім цього, існує класифікація кручених пар за кількістю пар, що згруповані в один кабель. Найбільш розповсюджений тип для використання в комп'ютерних мережах – це категорія CAT5, яка містить 4 пари дротів різних кольорів. Максимальна швидкість передачі даних становить до 1 Гб/с при використанні усіх пар [7].

Важливо розрізняти електричну ізоляцію провідників, присутню в кожному кабелі, від електромагнітної ізоляції. Перша представлена непровідним діелектричним шаром - папером або полімером, таким як полівінілхлорид чи полістирол. У другому випадку, крім електричної ізоляції, провідні жили захищені електромагнітним екраном, для створення якого зазвичай використовують мідне обплетення, що проводить [7].

Зкручування провідників здійснюється з метою збільшення рівня взаємозв'язку між провідниками однієї пари (електромагнітні перешкоди впливають на обидва проводи пари однаково) та для подальшого зниження електромагнітних перешкод з зовнішніх джерел і взаємних наведень при передачі диференціальних сигналів [7].

Екранована кручена пара ефективно захищає передані сигнали від зовнішніх перешкод і водночас зменшує випромінювання електромагнітних хвиль назовні, що допомагає захистити користувачів мережі від шкідливого

випромінювання. Проте наявність заземленого екрану робить кабель дорожчим та ускладнює його укладання.

Для створення мереж використовують такі типи кабелів:

- UTP (unshielded twisted pair) - неекранована кручена пара, де кручені пари не мають додаткового екранування (рис .1.6);

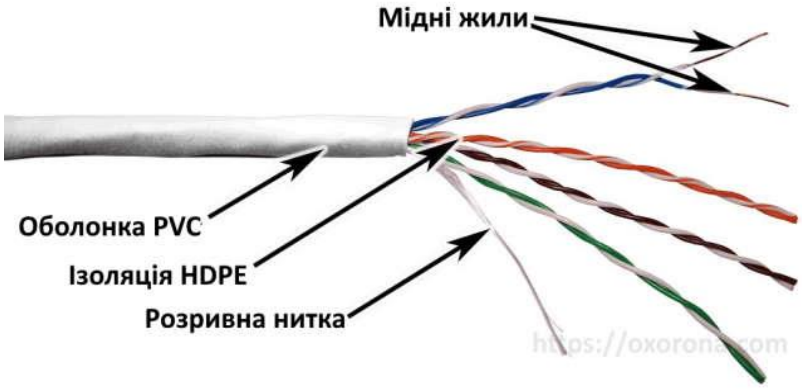

Рисунок 1.6 – Вита пара типу UTP

- FTP (Foiled Twisted Pair) - фольгована кручена пара - має спільний екран з фольги, однак у кожної пари немає індивідуального захисту (рис. 1.7);

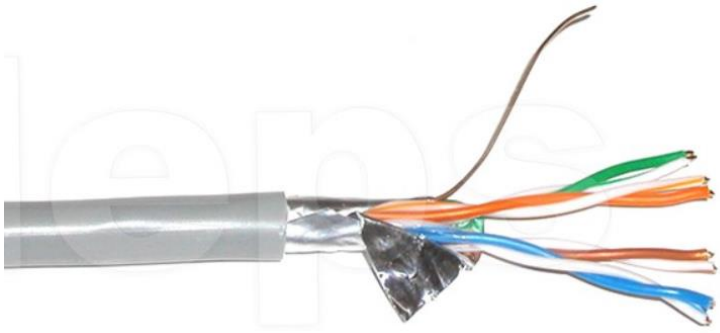

Рисунок 1.7 – Вита пара типу FTP

- STP (shielded twisted pair) - захищена кручена пара - кожна пара має власний екран (рис. 1.8);

Рисунок 1.8 – Вита пара типу STP

Переваги включають: легкість установки та доступну вартість. Основний недолік: велика вразливість до електромагнітних завад. Щоб обмежити вплив електромагнітних завад, застосовують екранування. В залежності від кількості скруток на метр, типу ізоляції та виду екрану розрізняють категорії кручених пар та їх частоту застосування: 3 категорія – 16МГц, 4 категорія – 20 МГц, 5 категорія – 100 МГц. Зазвичай довжина сегмента становить 100 метрів.

Категорії кабелів крученої пари

Існують різні категорії кабелів крученої пари, які вказують на ефективний діапазон частот, що пропускаються. Кабелі вищих категорій зазвичай містять більше пар проводів, і кожна пара має більше скруток на метр [7].

CAT1 (діапазон частот 0,1 МГц) - телефонний кабель, містить лише одну пару. Застосовується виключно для передачі голосу або даних через модем [7].

CAT2 (діапазон частот 1 МГц) - застарілий тип кабелю, має 2 пари провідників, підтримує передачу даних зі швидкістю до 4 Мбіт/с, використовувався в мережах Token Ring та Arcnet. Сьогодні іноді можна зустріти в телефонних мережах [7].

CAT3 (діапазон частот 16 МГц) - 4-парний кабель, застосовується для створення телефонних і локальних мереж 10BASE-T і token ring, підтримує швидкість передачі даних до 10 Мбіт/с або 100 МБіт/с за технологією 100BASE-T4 на відстань до 100 метрів. Відповідає стандарту IEEE 802.3, на відміну від попередніх категорій [7].

CAT4 (діапазон частот 20 МГц) - кабель складається з 4 скручених пар,

використовувався в мережах Token Ring, 10BASE-T, 100BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с на пару, наразі не застосовується [7].

CAT5 (діапазон частот 100 МГц) - 4-парний кабель, використовувався для створення локальних мереж 100BASE-TX і телефонних ліній, підтримує швидкість передачі даних до 100 Мбіт/с при використанні 2 пар [7].

CAT5e (діапазон частот 125 МГц) - 4-парний кабель, покращена версія категорії 5. Швидкість передачі даних до 100 Мбіт/с при використанні 2 пар і до 1000 Мбіт/с при використанні 4 пар. Кабель категорії 5e є найбільш розповсюдженим і застосовується для створення комп'ютерних мереж [7].

CAT6 (діапазон частот 250 МГц) - використовується в мережах Fast Ethernet та Gigabit Ethernet, складається з 4 пар провідників і може передавати дані зі швидкістю до 1000 Мбіт/с. Введений у стандарт у червні 2002 року [7].

CAT6a (діапазон частот 500 МГц) - застосовується в мережах Ethernet, складається з 4 пар провідників і може передавати дані зі швидкістю до 10 Гбіт/с і планується використовувати для додатків зі швидкістю до 40 Гбіт/с. Введений у стандарт у лютому 2008 року [7].

CAT7 - специфікація цього типу кабелю затверджена тільки міжнародним стандартом ISO 11801, швидкість передачі даних до 10 Гбіт/с, частота сигналу до 600-700 МГц. Кабель цієї категорії має загальний екран та індивідуальні екрани для кожної пари. Сьома категорія, строго кажучи, не UTP, а S/FTP (Screened Fully Shielded Twisted Pair) [7].

1.4.2 Оптоволокно

Оптоволоконний кабель, відомий також як волоконно-оптичний, представляє собою унікальний тип кабелю у порівнянні з іншими видами електричних або мідних кабелів. Відмінність полягає в тому, що передача інформації відбувається за допомогою світлового сигналу, а не електричного. Основний компонент - це прозоре волокно зі скла, через яке світло передається на значні відстані (до кількох десятків кілометрів) із мінімальним затуханням [7].

Волоконно-оптичний кабель складається з дрібних (5-60 мікрон) гнучких скляних волокон (оптичних світловодів), через які передаються світлові сигнали. Цей тип кабелю є найвищої якості - він дозволяє передавати дані з надзвичайно великою швидкістю (до 10 Гбіт/с і більше) і, крім того, краще

захищає дані від зовнішніх перешкод порівняно з іншими типами кабелів, завдяки особливостям розповсюдження світла, які дозволяють легко екранувати такі сигнали [7].

Кожне скляне волокно складається з центрального світлопроводу (серцевини) — скляного волокна, та скляної оболонки з меншим коефіцієнтом заломлення, ніж у серцевини. Світлові промені, розповсюджуючись через серцевину, не виходять за її межі, відбиваючись від оболонки [7].

Конструкція оптоволоконного кабелю є досить простою і нагадує структуру коаксіального електричного кабелю, але замість мідного проводу в центрі тут використовується тонке скловолокно (діаметром приблизно 1-10 мкм), а замість внутрішньої ізоляції - скляна або пластикова оболонка, яка запобігає виходу світла за межі волокна (рис. 1.9). Тут діє принцип так званого повного внутрішнього відбиття світла на межі двох середовищ з різними показниками заломлення (у скляній оболонці показник заломлення значно нижчий, ніж у центрального волокна). Металева оплітка кабелю зазвичай відсутня, оскільки захист від зовнішніх електромагнітних перешкод не є необхідним, але іноді її використовують для механічного захисту від зовнішнього середовища (такий кабель іноді називають броньованим, він може містити під однією оболонкою кілька оптоволоконних кабелів) [7].

Рисунок 1.9 – Структура оптичного кабелю

Зовнішні електромагнітні перешкоди не можуть вплинути на світловий сигнал, а сам сигнал не створює зовнішніх електромагнітних випромінювань. Однак, в цьому випадку потрібно використовувати спеціальні оптичні приймачі та передавачі, які перетворюють світлові сигнали в електричні і навпаки, що іноді значно підвищує загальну вартість мережі.

Зазвичай втрата сигналу в оптоволоконних лініях на частотах, що застосовуються у локальних мережах, складає приблизно 5 дБ/км, що є порівнянним з показниками електричних кабелів на низьких частотах.

Проте у використанні оптоволоконних кабелів існують певні складнощі. Основною проблемою є складний процес монтажу (для встановлення роз'ємів потрібна мікронна точність, а від точності обробки кінця волокна та якості його полірування значно залежить втрата сигналу в роз'ємі). Для монтажу роз'ємів використовують методи зварювання або склеювання з використанням спеціального гелю, індекс заломлення якого співпадає з індексом заломлення скловолокна. В будь-якому випадку це вимагає високої кваліфікації персоналу та спеціального обладнання. Таким чином, оптоволоконний кабель зазвичай продається у вигляді вже нарізаних сегментів різної довжини з вже встановленими на кінцях роз'ємами потрібного типу. В цьому випадку проблеми сумісності та заземлення відсутні. Кабель забезпечує ідеальну гальванічну ізоляцію між комп'ютерами мережі [7].

2 РОЗРАХУНОК ПРОПУСКНОЇ СПРОМОЖНОСТІ ПРОЄКТОВАНОЇ МЕРЕЖІ

2.1 Упорядкування логічної схеми мережі

Результуюча логічна схема мережі торгового центру представлена на рис. 2.1. Вихід в інтернет буде здійснюватися через маршрутизатор, також на ньому будуть прописані VLAN та правила доступу до інформації в мережі. Поверхи між собою та окремі приміщення з великою кількістю користувачів з'єднуються комутаторами, а робочі станції та клієнти підключаються до комутаторів офісу чи точок доступу відповідно. Банкомати торгового центру підключені до окремого комутатора. Для мережі відеоспостереження відведено окремий VLAN.

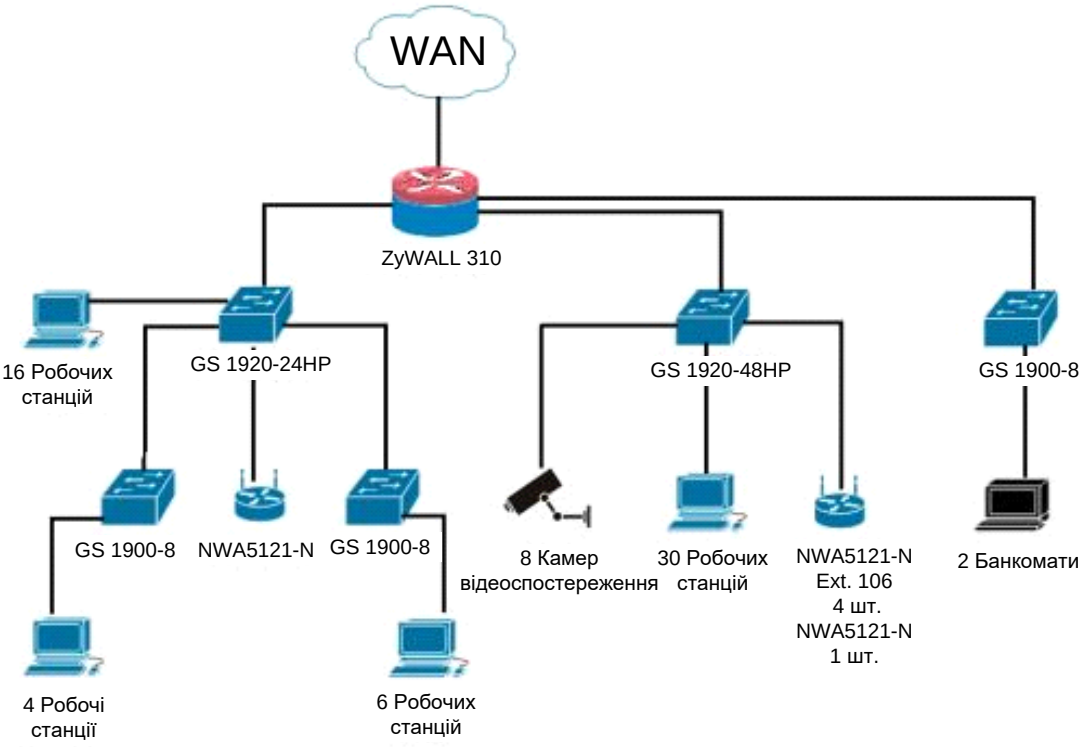

Рисунок 2.1 – Логічна схема мережі

Повна схема розташування мережевих пристроїв та прокладки кабелю на поверхах показана на рис. 2.2 – 2.4.

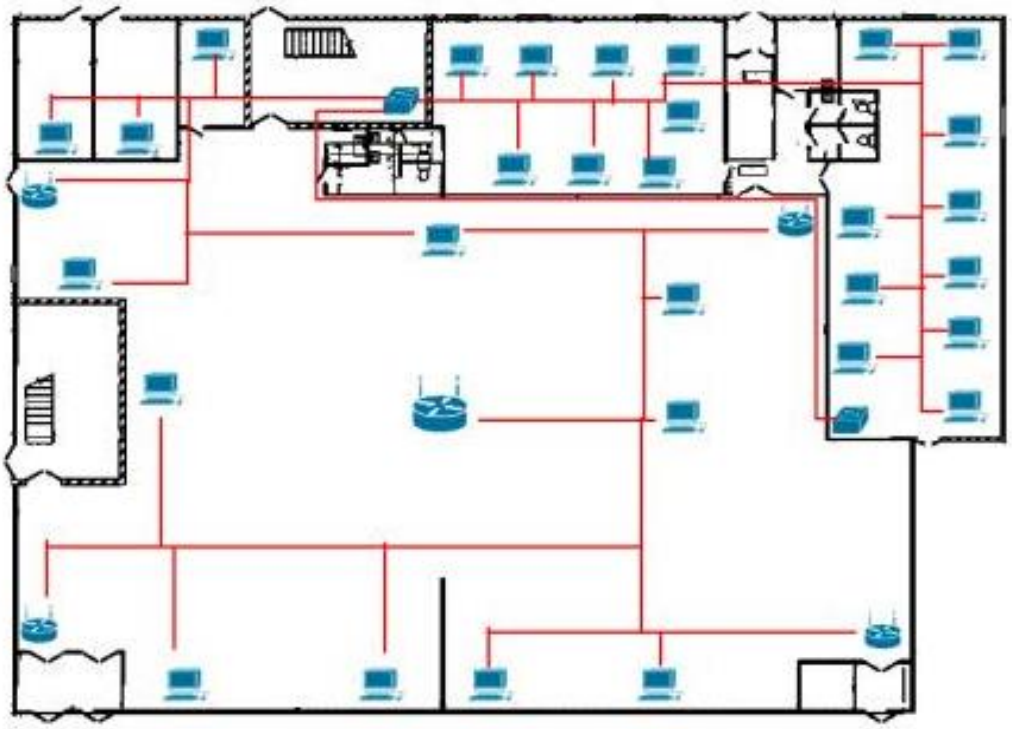

Рисунок 2.2 – Розташування елементів мережі (1 поверх)

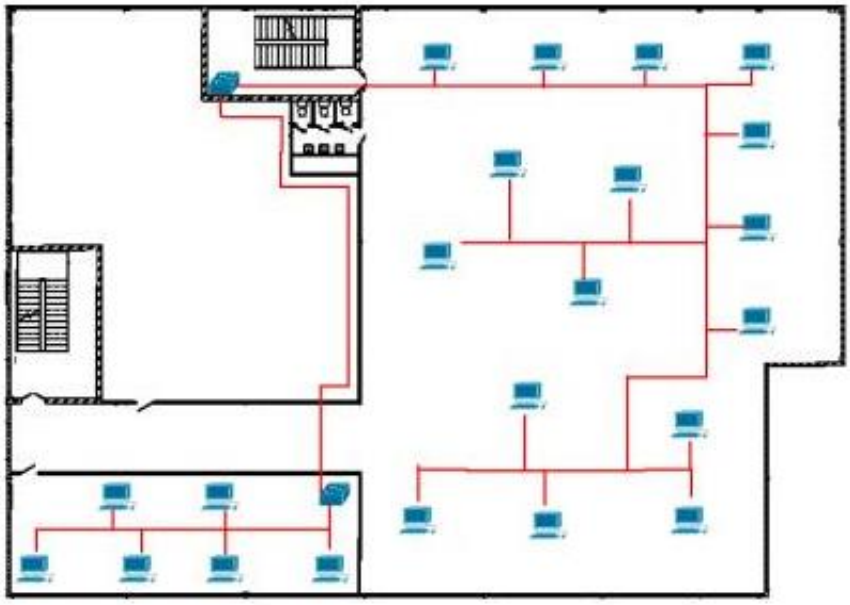

Рисунок 2.3 – Розташування елементів мережі (2 поверх)

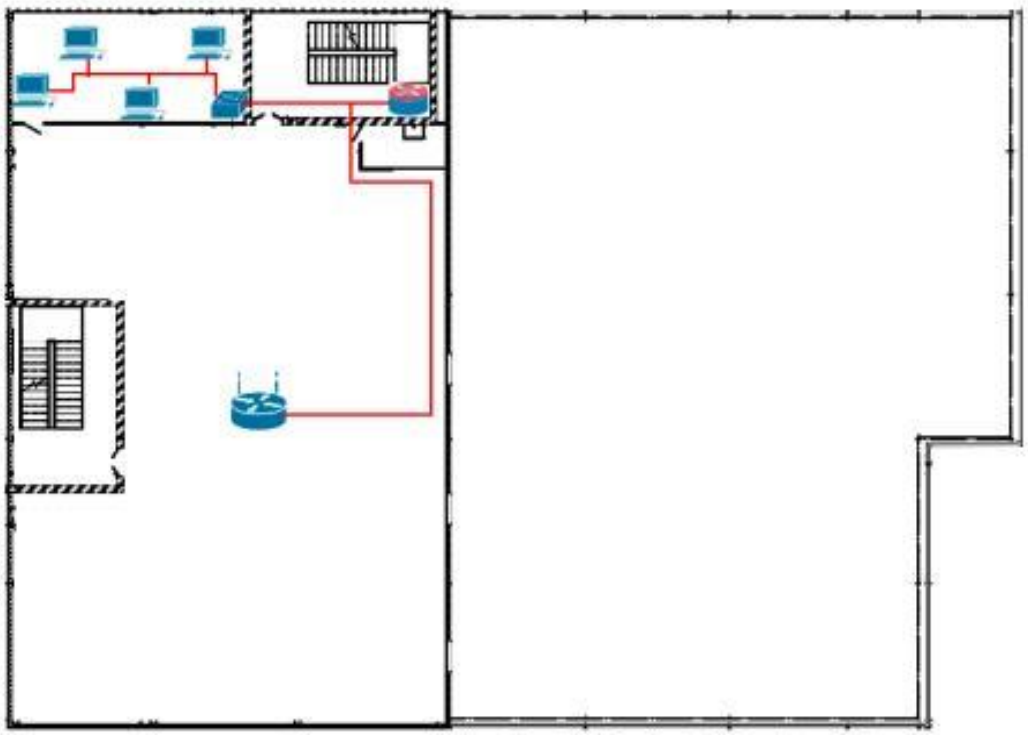

Рисунок 2.4 – Розташування елементів мережі (3 поверх)

З’єднання комутаторів між собою та користувачів з комутаторами буде реалізовано за допомогою витої пари категорії 5е. Підключення до зовнішньої мережі реалізовано через оптичний кабель. Структурована кабельна система в приміщенні організована за допомогою кабельросту під дахом кожного поверху. Головний маршрутизатор розміщено на третьому поверсі у антивандальній шафі, так як вхід провайдера у будинок відбувається через горище, будинок підключено до зовнішньої мережі через мережу PON і повітряну прокладку кабелю.

2.2 Організація VLAN

Для покращення роботи мережі та можливості керування трафіком необхідно розділення фізичної мережі на підрозділи, що найефективніше реалізувати через створення віртуальних локальних мереж VLAN.

Для розроблюваної мережі необхідно створити 6 VLAN у відповідності до різних підрозділів: адміністрація, банкомати, відеоспостереження, співробітники торгового залу, співробітники офісу, клієнти що підключаються

до гостьової бездротової мережі.

Таким чином діапазони IP-адрес сегментів мережі та відповідні VLAN можна побачити в таблиці 2.1. Перші IP-адреси в кожній підмережі буде відведено під адресу шлюзу на маршрутизаторі: 192.168.2.1, 192.168.3.1 і так далі.

Таблиця 2.1 – список VLAN-ів

VLAN Number	VLAN Name	Діапазон адрес користувачів	Mask
2	VLAN2	192.168.2.2 - 192.168.2.254	255.255.255.0
3	VLAN3	192.168.3.2 - 192.168.3.254	255.255.255.0
4	VLAN4	192.168.4.2 - 192.168.4.254	255.255.255.0
5	VLAN5	192.168.5.2 - 192.168.5.254	255.255.255.0
6	VLAN6	192.168.6.2 - 192.168.6.254	255.255.255.0
7	VLAN7	192.168.7.2 - 192.168.7.254	255.255.255.0

При реалізації локальної мережі (ЛМЗ) з використанням маршрутизатора, навіть за наявності фільтрів трафіку, мережа функціонує як єдиний широкомовний домен. Це означає, що широкомовні пакети розсилаються на всі пристрої в мережі. Комутатор в даному випадку не ізолює широкомовний трафік. Такі мережі називають "плоскими", оскільки вони не мають ієрархічної структури з точки зору широкомовних доменів.

Завдання передбачає створення шести віртуальних локальних мереж (VLAN) на маршрутизаторі третього рівня (L3), з призначенням кожної VLAN відповідним портам. На комутаторах другого рівня (L2) необхідно налаштувати відповідні VLAN. Для ефективного використання резервного каналу між комутаторами та маршрутизатором, пропонується налаштувати статичну агрегацію каналів (LAG). Це дозволить подвоїти пропускну здатність цього

з'єднання.

Проведемо налаштування L2 комутаторів, розглянемо на прикладі тільки 1 VLAN-у, так як воно буде ідентично для всіх (змінюватиметься тільки номер VLAN та діапазон IP-адрес).

Через командну консоль на комутаторі:

1. Входимо в режим глобального конфігурування:

```
en
conf t
```

2. Створюємо на комутаторі відповідний до підрозділу VLAN:

```
vlan 2
name VLAN2
exit
```

3. Призначаємо абонентським портам комутатора fa 0/1-24 відповідний VLAN:

```
int range fa 0/1-24
switchport mode access
switchport access vlan 2
exit
```

4. Підіймаємо на портах комутатора статичне агрегування каналів, створюємо відповідну групу каналів (наприклад група 1):

```
interface range gi 0/1-2
channel-group 1 mod on
exit
```

5. Створеній групі каналів прописуємо магістральний режим для можливості передачі даних іншим VLAN-ам та присвоюємо відповідний VLAN:

```
int port-channel 1
switchport mode trunk
switchport trunk allowed vlan 2
exit
```

6. Фіксуємо всі зміни в налаштуваннях:

```
end
write memory
```

Проведемо налаштування L3 маршрутизатора

Через командну консоль:

1. Входимо в режим глобального конфігурування:

```
en
conf t
```

2. Створюємо на маршрутизаторі всі шість VLAN-ів. Виконуємо по черзі для всіх VLAN-ів:

```
vlan 2
name VLAN2
exit
```

3. Кожному віртуальному порту, відповідальному за свій VLAN, присвоюємо індивідуальну IP-адресу (наприклад для VLAN2 IP-адреса 192.168.2.1). Виконуємо по черзі для всіх VLAN-ів:

```
int vlan 2
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
```

4. Підключаємо IP маршрутизацію:

```
ip routing
```

5. Створюємо групи каналів для всіх шести VLAN-ів, вказуємо протокол та підключаємо на них статичне агрегування (наприклад пара портів ge 1/0/1-2 група каналів 1) . Виконуємо по черзі для всіх шести груп каналів:

```
interface range gi 1/0/1-2
channel-protocol lacp
```

channel-group 1 mod on
exit

6. Кожній створеній групі каналів вказуємо тип інкапсуляції сигналу, прописуємо магістральний режим, та присвоюємо відповідний VLAN (наприклад для групи каналів 1 присвоюємо VLAN2). Виконуємо по черзі для всіх шести груп каналів:

int port-channel 1
switchport trunk encapsulation dot1q 2
switchport mode trunk
switchport trunk allowed vlan 2

7. Для деяких сегментів мережі необхідно встановлення певних правил передачі, в такому випадку створюються листи доступу, в яких ці правила будуть прописані, і відповідно до яких буде працювати маршрутизатор.

Призначення access-list у відповідності до номеру VLAN:
Router(config)#ip access-list standard 2
Router(config-std-nacl)#deny any
Router(config-std-nacl)#ex
Присвоєння сабінтерфейсу fa1/0 створеного access-list 2
Router(config)#int fa1/0
Router(config-if)#ip access-group 2 out
Router(config-if)#ex

2.3 Розрахунок показників локальної мережі

Мета роботи полягає у визначенні технічних параметрів локальної мережі, виборі необхідного апаратного та програмного забезпечення для локальної обчислювальної мережі (ЛОМ) організації, розподілі мережевих вузлів та каналів зв'язку, обчисленні економічних показників корпоративної локальної мережі.

Основою для проектування мережі служать:

- список задач та сервісів, які будуть виконуватися в мережі;

- кількість та місцезнаходження комп'ютерів – робочих станцій та серверів;

- план приміщень, де потрібно встановити локальну мережу;

- спеціальні технічні, економічні та експлуатаційні умови.

У процесі проектування вирішуються наступні завдання:

- вибір технології (технологій) передачі для мережі;

- обчислення та планування середнього обсягу трафіку та коефіцієнта завантаження мережі;

- визначення топології мережевих з'єднань;

- підбір необхідного мережевого обладнання та типу кабельної системи;

- створення схеми кабельної розводки та розташування робочих станцій та серверів.

Далі представлено порядок проектування ЛОМ.

Планування проекту ЛОМ розпочинається з попереднього визначення базової мережевої технології для розроблюваної локальної мережі на основі технічних вимог, експертних оцінок та теоретичних даних. У табл. 2.1 представлені найбільш розповсюджені технології сучасних локальних мереж.

Для кожного завдання встановлюється ефективність трафіку P_e і як співвідношення середнього часу обробки задачі мережею $t_{ср.і}$ (див. табл. 2.2) до загального часу функціонування мережі $t_{роб}$, що множиться на номінальну пропускну спроможність мережі $P_н$ у випадку її повного завантаження завданням або, при фіксованому трафіку, на його рівень [8].

Таблиця 2.1 – Технології локальних мереж

Специфікація	Номінальна пропускна спроможність	Топологія	Устаткування	Особливості
Ethernet 10Base-2	10 Мбіт/с	шина	мережні карти, коаксіальний кабель, Т-конектори, термінатори	дешевизна, невисока надійність
Ethernet 10Base-T	10 Мбіт/с	зірка, дерево	мережеві карти, кручена пара, концентратори (комутатори)	найпопулярніші технології, часто використовуються спільно
Fast Ethernet КП1	100 Мбіт/с	зірка, дерево	мережеві карти, кручена пара, концентратори (комутатори)	
Fast Ethernet ОВ2	100 Мбіт/с	точка-точка	мережеві карти, оптоволокно, комутатори	для з'єднання відділів (груп) або серверів
Gigabit Ethernet	1 Гбіт/с	точка-точка	оптоволокно, комутатори	
Radio Ethernet	11 Мбіт/с	зірка	мережні карти, точки доступу (концентратори)	використовується де прокладка кабелю нераціональна

1 КП – кручена пара; 2 ОВ – оптоволокно.

Таблиця 2.2 - Мережеві задачі, що використовуються в сучасних локальних мережах

Завдання	Середній час заняття мережею, хв. на добу.	Серверна частина	Клієнтська частина
обмін файлами	10-60 на 1 станцію	Мережева ОС	Мережева ОС
файловий сервер	120-360	Серверна мережева ОС	Клієнтська мережева ОС
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	Мережева ОС	Мережева ОС
мережевий друк	1-20 на 1 станцію	Мережева ОС	Мережева ОС
служба терміналів	10-300 на 1 станцію (трафік 14-100 кбіт/с)	Серверна мережева ОС	Клієнтська мережева ОС
СУБД	5-30 на 1 станцію	Сервер БД	Додатки БД
віддалений доступ	60-480 на 1 пару модемів	Сервер видав. доступу	Клієнт вилучив. доступу
Інтернет	10-120 на 1 клієнта	Проксі-сервер	Браузер
електронна пошта	0,5-2 на 1 клієнта	Поштовий сервер	Поштовий клієнт
Інтернет	5-20 на 1 клієнта	Веб-сервер	Браузер
інтерактивні повідомлення	1-5 на 1 станцію	різні	Різні
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	різні	Різні
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	різні	Різні
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	Серверна мережева ОС	Клієнтська мережева ОС

Отримані значення підсумовуються для визначення загального мережевого трафіку $P_{\Sigma}з$. Значення $P_{\Sigma}з$ множиться на коефіцієнт службового, широкомовного та неврахованого трафіку $k_{с.т.} = (0,05 \div 0,07) \cdot n$, де n – кількість комп'ютерів в мережі, та коефіцієнт запасу $k_з = (1,2 \div 2,0)$ для врахування майбутнього розвитку мережі.

Таблиця 2.3 - Розрахунок трафіку мережі

Завдання	Середній час заняття мережею, хв. на добу.	T	$T_{срі}$	P_{ie}
обмін файлами	10-60 на 1 станцію	10	620	93.939
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	5	310	46.97
мережевий друк	1-20 на 1 станцію	1	62	9.394
СУБД	5-30 на 1 станцію	5	310	1.515
Інтернет	10-120 на 1 клієнта	10	620	93.939
електронна пошта	0,5-2 на 1 клієнта	0.5	31	4.697
інтерактивні повідомлення	1-5 на 1 станцію	1	62	9.394
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	620	0.031
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	1240	0.188
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	930	140.909
				419.158

$$P_{\Sigma} = P_{\Sigma з} * k_{ст} * k_{з} = 419,16 * 0,05 * 62 * 1,2 = 1559,28 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 1559,28 / 100 = 15,6$$

На основі отриманого значення P_{Σ} проводиться корекція вибраної технології ЛОМ, щоб коефіцієнт ефективності мережі $k_{еф.} = P_{\Sigma} / P_{ном}$ був незначно вище (0,3÷0,6). Це передбачає зниження середнього часу виконання одного або декількох завдань, або ж використання іншої мережевої технології. Допускається збільшення загального часу роботи серверів завдяки використанню нічного періоду.

У випадку коли трафік перевищує норму, мережу ділять на логічні сегменти за допомогою комутаторів. Визначається загальний трафік для кожного логічного сегмента. Для кожного логічного сегмента переглядається коефіцієнт ефективності мережі. Якщо отриманий коефіцієнт ефективності мережі не задовольняє встановленим критеріям, мережу поділяють на декілька логічних мереж. Для них проводиться подібний розрахунок.

Розрахунок для VLAN 2 (табл. 2.4)

Висновок: Отримані значення коефіцієнта використання мережі для даного сегмента задовольняють нормі (0,3 ÷0,6).

Таблиця 2.4 - Розрахунок трафіку мережі для VLAN 2

Завдання	Середній час заняття мережею, хв. на добу.	T	$T_{срі}$	P_{ie}
обмін файлами	10-60 на 1 станцію	10	100	15.152
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	5	50	7.576
мережевий друк	1-20 на 1 станцію	1	10	1.515
СУБД	5-30 на 1 станцію	5	50	1.515
Інтернет	10-120 на 1 клієнта	10	100	15.152
електронна пошта	0,5-2 на 1 клієнта	0.5	5	0.758
інтерактивні повідомлення	1-5 на 1 станцію	1	10	1.515
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	100	0.05
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	200	0.03
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	150	22.727
				84.126

$$P_{\Sigma} = P_{\Sigma з} * k_{ст} * k_{з} = 84,126 * 0,05 * 10 * 1,2 = 50,5 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 50,5/100 = 0,505$$

Розрахунок для VLAN 3 (табл. 2.5)

Таблиця 2.5 – Розрахунок трафіку мережі для VLAN 3

Завдання	Середній час заняття мережею, хв. на добу.	T	T_{cpi}	P_{ie}
обмін файлами	10-60 на 1 станцію	10	100	15.152
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	5	50	7.576
мережевий друк	1-20 на 1 станцію	1	10	1.515
СУБД	5-30 на 1 станцію	5	50	1.515
Інтернет	10-120 на 1 клієнта	10	100	15.152
електронна пошта	0,5-2 на 1 клієнта	0.5	5	0.758
інтерактивні повідомлення	1-5 на 1 станцію	1	10	1.515
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	100	0.05
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	200	0.03
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	150	22.727
				84.126

$$P_{\Sigma} = P_{\Sigma З} * k_{ст} * k_{з} = 84,126 * 0,05 * 10 * 1,2 = 50,5 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 50,5/100 = 0,505$$

Висновок: Отримані значення коефіцієнта використання мережі для даного сегмента задовольняють нормі (0,3 ÷0,6).

Розрахунок для VLAN 4 (табл. 2.6)

Таблиця 2.6 - Розрахунок трафіку мережі для VLAN 4

Завдання	Середній час заняття мережею, хв. на добу.	T	T_{cpi}	P_{ie}
обмін файлами	10-60 на 1 станцію	10	100	15.152
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб.	5	50	7.576
мережевий друк	1-20 на 1 станцію	1	10	1.515
СУБД	5-30 на 1 станцію	5	50	1.515
Інтернет	10-120 на 1 клієнта	10	100	15.152
електронна пошта	0,5-2 на 1 клієнта	0.5	5	0.758
інтерактивні повідомлення	1-5 на 1 станцію	1	10	1.515
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	100	0.05
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	200	0.03
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	150	22.727
				84.126

$$P_{\Sigma} = P_{\Sigma З} * k_{ст} * k_{з} = 84,126 * 0,05 * 10 * 1,2 = 50,5 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 50,5/100 = 0,505$$

Висновок: Отримані значення коефіцієнта використання мережі для даного сегмента задовольняють нормі (0,3 ÷0,6).

Розрахунок для VLAN 5

Таблиця 2.7 – Розрахунок трафіку мережі для VLAN 5

Завдання	Середній час заняття мережею, хв. на добу.	T	T_{cpi}	P_{ie}
обмін файлами	10-60 на 1 станцію	10	100	15.152
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	5	50	7.576
мережевий друк	1-20 на 1 станцію	1	10	1.515
СУБД	5-30 на 1 станцію	5	50	1.515
Інтернет	10-120 на 1 клієнта	10	100	15.152
електронна пошта	0,5-2 на 1 клієнта	0.5	5	0.758
інтерактивні повідомлення	1-5 на 1 станцію	1	10	1.515
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	100	0.05
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	200	0.03
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	150	22.727
				84.126

$$P_{\Sigma} = P_{\Sigma З} * k_{ст} * k_{з} = 84,126 * 0,05 * 10 * 1,2 = 50,5 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 50,5/100 = 0,505$$

Висновок: Отримані значення коефіцієнта використання мережі для даного сегмента задовольняють нормі (0,3 ÷0,6).

Розрахунок для VLAN 6 (табл. 2.8)

Таблиця 2.8 – Розрахунок трафіку мережі для VLAN 6

Завдання	Середній час заняття задачею мережі, хв.	T	T_{cpi}	P_{ie}
обмін файлами	10-60 на 1 станцію	10	110	16.667
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	5	55	8.333
мережевий друк	1-20 на 1 станцію	1	11	1.667
СУБД	5-30 на 1 станцію	5	55	1.515
Інтернет	10-120 на 1 клієнта	10	110	16.667
електронна пошта	0,5-2 на 1 клієнта	0.5	5.5	0.833
інтерактивні повідомлення	1-5 на 1 станцію	1	11	1.667
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	110	0.055
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	220	0.033
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	165	25
				90.569

$$P_{\Sigma} = P_{\Sigma З} * k_{ст} * k_{з} = 90,569 * 0,05 * 10 * 1,2 = 59,8 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 59,8/100 = 0,598$$

Висновок: Отримані значення коефіцієнта використання мережі для

даного сегмента задовольняють нормі (0,3 ÷0,6).

Розрахунок для VLAN 7 (табл. 2.9)

Таблиця 2.9 – Розрахунок трафіку мережі для VLAN 7

Завдання	Середній час заняття мережею, хв. на добу.	T	T_{cpi}	P_{ie}
обмін файлами	10-60 на 1 станцію	10	110	16.667
файловий сервер	120-360	120	120	18.182
резервування інформації	5-30 на 1 роб. станцію 10-120 на 1 сервер	5	55	8.333
мережевий друк	1-20 на 1 станцію	1	11	1.667
СУБД	5-30 на 1 станцію	5	55	1.515
Інтернет	10-120 на 1 клієнта	10	110	16.667
електронна пошта	0,5-2 на 1 клієнта	0.5	5.5	0.833
інтерактивні повідомлення	1-5 на 1 станцію	1	11	1.667
голосовий зв'язок (IP-телефонія)	10-60 на 1 станцію (трафік 33-64 кбіт/с)	10	110	0.055
Відеоконференції	20-40 на 1 станцію (трафік 0,1-1 Мбіт/с)	20	220	0.033
служби мережевої безпеки	15-20 на 1 сервер + 2-5 на 1 клієнта	15	165	25
				90.569

$$P_{\Sigma} = P_{\Sigma З} * k_{ст} * k_{з} = 90,569 * 0,05 * 10 * 1,2 = 59,8 \text{ Мбіт/с}$$

$$k_{еф.} = P_{\Sigma} / P_{ном} = 59,8/100 = 0,598$$

Висновок: Отримані значення коефіцієнта використання мережі для даного сегмента задовольняють нормі (0,3 ÷0,6).

3 ВИБІР ОБЛАДНАННЯ ДЛЯ ПРОЄКТОВАНОЇ МЕРЕЖІ

3.1 Вибір міжмережного екрану

Таблиця 3.1 – Порівняння міжмережних екранів

Найменування	D-link DFL-1660	ZyXEL ZyWALL 310
Тип пристрою	маршрутизатор (router)	маршрутизатор (router)
Кількість портів	6	8
Базова швидкість передачі даних	10/100/1000 Мбіт/сек	10/100/1000 Мбіт/сек
DHCP-сервер	є	є
Міжмережевий екран (Firewall)	є	є
NAT	є	є
SPI	ні	є
Підтримка Dynamic DNS	ні	є
Демілітаризована зона (DMZ)	є	є
WAN-порт	Ethernet 10/100/1000 Мбіт/сек	Ethernet 10/100/1000 Мбіт/сек
Пропускна спроможність (мбіт/с)	4900	6050
Підтримка VPN (VPN pass through)	є	є
Підтримка VPN-тунелів (VPN Endpoint)	є	є
Число підтримуваних VPN-тунелів	100	
Підтримка IPv6	ні	є
Об'єм оперативної пам'яті (Мб)		2G
Об'єм флеш-пам'яті (Мб)		512
Консольний порт	є	є
Web-інтерфейс	є	є
Підтримка Telnet	є	є
Підтримка SNMP	є	є
Підтримка RIP v1	ні	є
Підтримка RIP v2	ні	є
Підтримка IGMP v1	є	ні
Підтримка IGMP v2	є	ні
Підтримка IGMP v3	є	ні
Автоматичне визначення MDI/MDIX	є	є
Підтримка IEEE 802.1q (VLAN)	є	є
USB-порт	є	є

Міжмережевий екран ZyWALL 310 (рис .3.1) володіє всіма потрібними властивостями для створення мережевої безпеки в торговельному центрі. Він також коштує менше та має вищу пропускну здатність порівняно з DFL-1660.

Міжмережевий екран ZyWALL 310 розроблено для виконання різноманітних завдань у сфері створення корпоративних мереж з географічним розподілом будь-якого рівня складності та забезпечення комплексного захисту інфраструктури від інтернет-загроз [8].

Рисунок 3.1 - Міжмережевий екран ZyWALL 310 з вісьма гігабітними інтерфейсами, що конфігуруються

У відповідь на потреби глобалізації та мобільності бізнес-процесів, ZyWALL 310 оснащений розширеним набором функцій для створення захищених високошвидкісних VPN-каналів для з'єднання з філіями, партнерами та мобільними працівниками. Завдяки впровадженим у ZyWALL 310 VPN-технологіям, таким як IPSec, L2TP/IPSec і SSL, компанії мають можливість об'єднати свої розкидані підрозділи в єдину інформаційну систему, а також надати можливість роботи співробітникам на відстані. Надійний зв'язок з філіями забезпечується за допомогою резервування VPN-тунелів через різноманітні широкосмугові інтернет-канали, підключені до зовнішніх інтерфейсів апарату [8].

Сервіси мережевої безпеки UTM, інтегровані в ZyWALL 310, включаючи потоковий антивірус, систему виявлення та нейтралізації вторгнень, фільтрацію контенту, захист від спаму, моніторинг додатків та перевірку SSL-трафіку, забезпечують високий рівень безпеки мережі, захищаючи всю інфраструктуру компанії від зовнішніх загроз [8].

ZyWALL 310 базується на сучасній апаратній платформі з використанням потужного шестиядерного процесора Cavium Octeon II та перевіреної часом операційної системи ZLD, чия надійність та ефективність доведені багаторічним досвідом використання міжмережевих бар'єрів ZyWALL різними організаціями у всьому світі. Це забезпечує ZyWALL 310 одними з найкращих показників пропускної спроможності SPI Firewall та VPN у своєму класі [8].

Крім високої продуктивності в каналах VPN, міжмережевий екран ZyWALL 310 надає потужні інструменти для пріоритизації трафіку та розподілу пропускної здатності, відповідаючи таким чином на потреби бізнесу

у використанні сучасних додатків, чутливих до затримок і втрат даних. Таким чином, доступ до документів та баз даних стає можливим для співробітників віддалених філій [8].

Незважаючи на широкий спектр функціональних можливостей, міжмережеві екрани серії ZyWALL вирізняються компактністю, простотою у використанні та надійністю, пропонуючи привабливе співвідношення ціни та якості. Їх впровадження та обслуговування не вимагає значних фінансових чи трудових витрат [8].

Сервіси UTM

Антивірус у реальному часі, створений на основі передових технологій ZyXEL, активно сканує веб-трафік, блокуючи вхід шкідливих програм до корпоративної мережі. Система виявлення та протидії вторгненням (IDP) ефективно зупиняє мережеві черв'яки, троянські програми, бекдори, DoS та DDoS атаки, а також експлойти, які цілять уразливості ОС та застосунків.

Фільтрація контенту на основі CYREN технологій дозволяє обмежити доступ до сайтів з потенційною загрозою та тих, що не стосуються робочих завдань. Система фільтрації спаму захищає від небажаних та потенційно небезпечних електронних листів, шкідливого ПЗ та витоку конфіденційної інформації.

IPv6

Шлюзи підтримують протокол IPv6, що демонструють результати тестувань за програмою сертифікації IPv6 Gold Logo Phase 1 та Phase 2, ініційованої IPv6 Forum.

QoS

Пристрій дозволяє встановлювати пріоритети для різних типів мережевого трафіку за допомогою маркерів DSCP, забезпечуючи або обмежуючи пропускну спроможність. Історія розподілу пропускної спроможності фіксується та доступна для перегляду у вигляді звітів.

Підтримка Microsoft Active Directory

Функція Single Sign-on (SSO) для автентифікації користувачів MSAD на USG забезпечує безперервну автентифікацію.

Інспекція SSL

Функція інспекції SSL дешифрує SSL-трафік на ZyWALL для аналізу згаданими сервісами, після чого знову шифрує його перед передачею

одержувачу.

VPN та безпека

Окрім стандартної підтримки VPN через IPSec, також доступні L2TP over IPSec та SSL. Розумна система обробки правил визначає маршрутизацію пакетів згідно з політиками доступу, базуючись на різноманітних критеріях. Шлюз підтримує L3 віртуалізаційні технології: VLAN та віртуальні інтерфейси-псевдоніми, дозволяючи легко керувати безпекою різних відділів.

Безперервний доступ до Інтернету

Використання декількох WAN портів забезпечує резервування та балансування Інтернет-каналів, автоматичне перемикання на резервний канал при відмові основного та повернення до нього після відновлення, а також використання 3G/4G-модему як резервного каналу для забезпечення неперервного доступу до Інтернету.

Резервування пристрою

Функція резервування пристрою (Device HA) забезпечує неперервну роботу за допомогою використання двох шлюзів: основного та резервного.

USB порт для розширення можливостей

USB порти можна використовувати для підключення 3G-модемів та FLASH-накопичувачів для зберігання логів та захоплених дампів трафіку.

Вмонтований керуючий модуль Wi-Fi точок доступу

Вбудований керуючий модуль для Wi-Fi точок доступу через CAPWAP дозволяє централізовано керувати двома точками доступу серії NWA від ZyXEL без потреби у додаткових картах розширення.

Карти розширення

Карти для підключення сервісу управління Wi-Fi точками доступу для ZyWALL та USG. Карта для додавання SSL VPN тунелів

Програми

Програма Vantage Report 3 для генерації звітів та обліку трафіку призначена для централізованого збирання, збереження, аналізу та обробки даних про роботу розподіленої мережі безпекових пристроїв ZyXEL.

Програмні VPN-клієнти IPSec та SSL для Windows

3.2 Вибір комутаторів

Під час вибору комутатора для організації мережі одним з ключових критеріїв є наявність підтримки технології VLAN (802.1q) комутатором.

Термін VLAN (Virtual LAN) використовують для позначення групи мережевих вузлів, які формують окремий домен для широкомовного трафіку (Broadcast Domain). Це визначення точне, проте не надто інформативне, тому давайте розглянемо суть віртуальних мереж детальніше [2].

У випадку створення локальної мережі за допомогою комутатора, незалежно від можливості застосування фільтрації трафіку для користувачів, усі вузли мережі становлять єдиний домен для широкомовного трафіку, тобто такий трафік розповсюджується на всі вузли мережі. Отже, за замовчуванням комутатор не обмежує широкомовний трафік, а мережі, побудовані за цим принципом, називають плоскими [2].

Віртуальні мережі створюють групу мережевих вузлів, в якій весь трафік, включно з широкомовним, ізольований на канальному рівні від інших вузлів мережі. Це означає, що обмін кадрами між вузлами мережі, які належать до різних віртуальних мереж, на основі канальної адреси є неможливим (при цьому віртуальні мережі можуть взаємодіяти між собою на мережному рівні через маршрутизатори) [2].

Застосування технології віртуальних мереж для ізоляції окремих вузлів мережі на канальному рівні дозволяє одночасно вирішувати декілька завдань. З одного боку, віртуальні мережі допомагають збільшити продуктивність мережі, локалізуючи широкомовний трафік у межах однієї віртуальної мережі та створюючи перешкоду для широкомовного шторму. Комутатори передають широкомовні пакети (а також пакети з груповими та невідомими адресами) лише в межах однієї віртуальної мережі, але не між різними віртуальними мережами. З іншого боку, ізоляція віртуальних мереж між собою на канальному рівні сприяє збільшенню безпеки мережі, обмежуючи доступ до певних ресурсів для окремих категорій користувачів [2].

Кваліфікаційна робота передбачає використання комутаторів з різною кількістю портів.

Таблиця 3.2 - Порівняння комутаторів

Виробник	Cisco	ZyXEL	D-link
Модель	SF500-24P	GS1920-24HP	DES-3528
Можливість встановлення у стійку	є	є	є
Кількість слотів для додаткових інтерфейсів	2	4	2
Об'єм оперативної пам'яті (Мб)	8	64	
Об'єм флеш-пам'яті (Мб)		16	
Додатково			
Автоматичне визначення MDI/MDIX	є	є	є
Підтримка Power over Ethernet	є	є	ні
Підтримка Jumbo Frame	є	ні	є
Підтримка IEEE 802.1p (Priority tags)	Є	є	є
Підтримка IEEE 802.1q (VLAN)	є	є	є
Підтримка IEEE 802.1d (Spanning Tree)	є	є	є
Підтримка IEEE 802.1s (Multiple Spanning Tree)	є	є	є
Підтримка IPv6	є	є	є
Ширина (мм)	440	438	441
Висота (мм)	44	44	44
Глибина (мм)	257	200	210
Вага (кг)	3,73 кг	2,6 кг	2,51 кг
LAN			
Кількість портів	24	24	24
Базова швидкість передачі даних	10/100 Мбіт/сек	10/100 Мбіт/сек	10/100 Мбіт/сек
Внутрішня пропускна здатність (Гбіт/сек)	28.8	52.8	12.8
Кількість uplink/стек/SFP-портів та модулів	2	4	2
Максимальна швидкість uplink/SFP-портів	10/100/1000 Мбіт/сек	10/100/1000 Мбіт/сек	10/100/1000 Мбіт/сек
Розмір таблиці MAC адрес	16384	16384	16384
Підтримка роботи у стеку	є	ні	є
Статична маршрутизація	є	є	є
Управління			
Консольний порт	є	є	є
Web-інтерфейс	є	є	є
Підтримка Telnet	є	є	є
Підтримка SNMP	є	є	є
Підтримка RIP v1	є	є	ні
Підтримка RIP v2	є	є	ні
Підтримка IGMP v1	є	є	є
Підтримка IGMP v2	є	є	є
Підтримка IGMP v3	є	є	є

В роботі обрано комутатор GS1920-24HP (рис. 3.2) тому що він має більш високу пропускну здатність та велику кількість додаткових портів.

Рисунок 3.2 – Зовнішній вигляд комутатора GS1920-24HP

Інтелектуальний High Power PoE-комутатор Gigabit Ethernet з 24 роз'ємами RJ-45 та 4 SFP-слотами поєднаними з роз'ємами RJ-45

Лінійка 1920 включає в себе гігабітні світчі, які підтримують як трансляцію даних, так і передачу даних разом з електроживленням через PoE (Power over Ethernet). Розроблені для використання на рівні доступу в малих та середніх компаніях, ці пристрої забезпечують захист від неавторизованого доступу, встановлення пріоритетів для відеотрафіку та VoIP, а також дозволяють керувати підключеннями клієнтів на рівні окремих портів. Всі моделі відповідають вимогам сучасних стандартів з енергоефективності IEEE802.3az [9].

Світчі з лінійки 1920 відносяться до категорії розумних світчів. Їх первинна настройка та подальше управління можливі через веб-інтерфейс або за допомогою протоколу SNMP з використанням груп моніторингу RMON. Технологія ZyXEL iStacking дозволяє управляти декількома світчами під однією IP-адресою. Функціонал LLDP дозволяє світчам інформувати локальну мережу про своє існування та специфікації, а також отримувати подібну інформацію від сусідніх світчів. Збір та аналіз даних про неполадки в мережі відбувається через Syslog або SNMP Trap [9].

Налаштування пріоритетів PoE

Кожен порт світча можна налаштувати для оптимальної подачі живлення PoE до підключеного мережевого обладнання. Адміністратор має змогу встановлювати часові рамки для активації та деактивації портів PoE, а також виділяти необхідну потужність для кожного пристрою з урахуванням його пріоритету та загального бюджету потужності PoE. У випадку, коли доступна

потужність наближається до свого максимуму, живлення припиняється для пристроїв з нижчим пріоритетом [9].

Списки контролю доступу

Списки контролю доступу ACL забезпечують високий рівень захисту передаваних даних. Трафік поділяється на потоки за певними критеріями, такими як IP-адреса відправника, IP-адреса отримувача, порт відправника та порт отримувача. Використовуючи встановлені критерії, можна фільтрувати або обмежувати швидкість для визначеного трафіку [9].

Протокол виявлення мережевих пристроїв

Протокол виявлення на канальному рівні LLDP (Link Layer Discovery Protocol) дозволяє мережевим пристроям анонсувати свою присутність та можливості іншим пристроям у локальній мережі. Він також дозволяє зберігати та оновлювати інформацію про пристрої, які безпосередньо підключені. Це сприяє адмініструванню мережі, дозволяючи адміністратору відстежувати зміни в мережі та своєчасно реагувати на них [9].

Утиліта налаштування ZON

Утиліта ZON уможливлює виявлення та налаштування світчів у мережі. Адміністраторам достатньо підключити обладнання до мережі, і вони з'являться в інтерфейсі ZON. Використовуючи цей інтерфейс, можна змінювати паролі, оновлювати ПЗ, перезавантажувати світчі та виконувати інші масові операції. ZON значно спрощує процес налаштування та скорочує час, необхідний для цього [9].

Пріоритизація трафіку

Однією з ключових вимог до сучасних мереж є пріоритизація трафіку для забезпечення безперебійної роботи сервісів, таких як відеоконференції та онлайн-освіта. Це досягається за допомогою управління якістю обслуговування (QoS), що передбачає забезпечення мінімальної затримки передачі даних та методи управління пропускною спроможністю мережі [9].

Протокол IPv6

Підтримка протоколів IPv6 забезпечує ефективну роботу в сучасних мережах передачі даних, дозволяючи налаштовувати та адмініструвати світч, забезпечувати захист і пріоритизацію трафіку, а також блокувати несанкціоновані підключення. Для роботи в мережах, що підтримують як IPv4, так і IPv6, передбачено використання стеку протоколів [9].

3.3 Вибір точки доступу

При виборі точки доступу враховується, що вона працюватиме у режимі Multi SSid. Тобто необхідно забезпечити функцію, що дозволяє одній точці доступу транслювати кілька бездротових мереж, кожна з яких має свій унікальний SSID (Service Set Identifier), тобто ім'я мережі. Це означає, що на одному пристрої можна створити кілька віртуальних бездротових мереж з різними налаштуваннями безпеки, що дозволяє розділити доступ для різних користувачів або цілей.

Таблиця 3.3 - Порівняння точок доступу

Найменування	D-link DAP-2690	ZyXEL NWA1123-ACv3	Cisco AIR-CAP2602E
Тип зв'язку	Wi-Fi	Wi-Fi	Wi-Fi
Частотний діапазон пристроїв Wi-Fi	2.4/5 ГГц	2.4/5 ГГц	2.4/5 ГГц
Стандарт Wi-Fi	802.11n	802.11n/ac	802.11n
Макс. швидкість бездротового з'єднання (Мбіт/с)	300	300/1200	450
Підтримка MIMO	є	є	є
Метод шифрування даних WPA	є	є	є
Метод шифрування даних WPA2	є	є	є
Підтримка 802.1x	ні	є	є
Кількість портів комутатора	1	1	1
Швидкість портів	1000 Мбіт/сек	1000 Мбіт/сек	1000 Мбіт/сек
Гостьова мережа	є	є	ні
Режим мосту	є	є	ні
Web-інтерфейс	є	є	є
Консольний порт	ні	є	є
Підтримка IEEE 802.1q (VLAN)	ні	є	ні
Підтримка SNMP	є	є	ні
Підтримка Telnet	є	є	ні
Кількість зовнішніх антен	4	4	4
Тип зовнішньої антени	знімна	знімна	знімна
Потужність передавача (dBM)	18	28	23
Підтримка Power over Ethernet	є	є	є
Ширина (мм)	191	198	221
Висота (мм)	37	45	54
Глибина (мм)	191	138	221
Вага (г)	990	462	1040

Виходячи з порівняння обираємо точку доступу ZyXEL NWA1123-ACv3 (рис. 3.3), що має необхідний набір характеристик для встановлення в торговому центрі.

Wi-Fi 802.11b/g/n/ac точка доступу, яка може працювати як незалежно, так і під управлінням контролера, може бути оснащена додатково зовнішніми антенами та підтримує технологію Tx Beamforming.

Точка доступу ZyXEL NWA1123-ACv3 використовує стандарт 802.11n або 802.11ac, забезпечуючи швидкість передачі даних до 1200 Мбіт/с, а також використовує технологію адаптивного формування діаграми спрямованості (Transmit Beamforming) для покращення радіопокриття [10].

Рисунок 3.3 – Зовнішній вигляд точки доступу ZyXEL NWA1123-ACv3

Забезпечення високого рівня безпеки бездротової мережі досягається за допомогою сучасних методів захисту, включаючи автентифікацію користувачів через сервер RADIUS, фільтрацію за MAC-адресами, Layer-2 Isolation, а також підтримку протоколів IEEE 802.1x, Wi-Fi Protected Access (WPA) і WPA2. NWA1123-ACv3 дозволяє створювати до 8 SSID для різних бездротових мереж і тегувати їх трафік за допомогою VLAN 802.1Q для забезпечення якості обслуговування [10].

SMA роз'єм для підключення зовнішньої антени надає можливість мережевому адміністратору використовувати антени MIMO 2,4 ГГц з будь-якою діаграмою спрямованості для налаштування необхідного радіопокриття. Точка доступу поставляється з комплектом для монтажу на стелю або стіну

[10].

NWA1123-ACv3 ідеально підходить для створення захищених корпоративних мереж на основі стандарту Wi-Fi 802.11n/ac, як у режимі управління контролером, так і в автономному режимі, особливо для автоматизації роботи на складах [10].

Підтримка 802.11n/ac

Підтримка стандарту 802.11n та 11ac і технології MIMO 2T2R з двома просторовими потоками даних дозволяє досягти максимальної швидкості бездротового зв'язку 300/1200 Мбіт/с [10].

Знімні антени

Точка доступу оснащена можливістю підключати знімні всеспрямовані антени з коефіцієнтом посилення 3 dBi. Завдяки знімним антенам, при необхідності можна підключити антени з більшим коефіцієнтом підсилення або MIMO антену з секторною діаграмою спрямованості, наприклад, ANT1314 [10].

Уніфікована точка доступу

При створенні невеликої бездротової мережі точки доступу серії NWA1123 можуть використовуватися в автономному режимі, з індивідуальним налаштуванням через графічний веб-інтерфейс. Для централізованого налаштування групи автономних точок доступу існує програма ZyXEL AP Configurator (ZAC), яка полегшує розгортання мережі. Автономні точки доступу можна в будь-який час переконфігурувати в режим управління для створення Wi-Fi мережі під керівництвом апаратного контролера. Серію NWA1123 можна інтегрувати з контролерами бездротових мереж серії NXC, а також з хот-спотами та шлюзами безпеки ZyXEL, які мають функцію контролера [10].

Інтерфейс Gigabit Ethernet

Для використання всіх переваг швидкості стандарту 802.11n/ac, точка доступу оснащена портом Gigabit Ethernet, що підтримує стандарт мережевого живлення 802.3af [10].

Корпус класу Plenum

Корпус точок доступу серії NWA1123 виготовлено з нетоксичних матеріалів без вмісту галогенів (Low Smoke Zero Halogen, LS0H) [10].

Протокол IPv6

Підтримка базових протоколів IPv6 забезпечує сумісність точки доступу з

сучасними мережами передачі даних [10].

ZyXEL AP Configurator

Точки доступу ZyXEL мають зручний веб-інтерфейс для повного управління пристроєм і контролю за роботою Wi-Fi мережі. Програма ZyXEL AP Configurator (ZAC) призначена для централізованого налаштування групи автономних точок доступу, спрощуючи розгортання масштабної бездротової мережі [10].

Також обираємо додаткову антену спрямованої дії. У нашому випадку це антена Ext 106 (рис. 3.4).

Рисунок 3.4 – Додаткова антена Ext 106 2.4 ГГц 6dBi спрямованої дії

Мікросмужковий (patch) тип антени з секторальною діаграмою напрямленості та коефіцієнтом підсилення 6 дБі. EXT-106 можлива бути з'єднана з офісними точками доступу через роз'єм RP-SMA, який працює на частоті 2,4 ГГц. Антена вирізняється компактними габаритами та легкою вагою. Встановлення EXT-106 є простим: можна монтувати як у вертикальній, так і в горизонтальній позиції, існує можливість регулювання кута нахилу антени відносно її кріплення. За допомогою кабелю подовження антену можна розмістити на певній відстані від точки доступу або Wi-Fi адаптера [10].

Основні переваги [10]:

- дальність передачі даних до 750 м при двоточковому з'єднанні з антенами EXT-106;

- компактні розміри, можливість горизонтального та вертикального

монтажу дозволяють розмістити антену в місцях, де досягається максимальна якість та дальність зв'язку з віддаленими користувачами.

Технічні характеристики:

- робочий діапазон частот 2,4 – 2,5 ГГц;
- роз'єм RP-SMA (female);
- кабель розширення 1,5 м;
- коефіцієнт підсилення 6 дБі;
- коефіцієнт стоячої хвилі (VSWR) максимум 1,5;
- поляризація лінійна вертикальна;
- ширина діаграми спрямованості горизонталлю 80°;
- ширина діаграми спрямованості за вертикаллю 80°;
- опір 50 Ом;
- розмір: 118 х 86 х 76 мм;
- маса 0,11 кг;
- температура довкілля під час роботи -10 °С – 55 °С;
- робоча вологість 95 % при 25 °С.

Рекомендовано для використання в ситуаціях організації двоточкових зв'язків, наприклад, для з'єднання двох офісів у єдину локальну мережу.

З'єднання віддалених користувачів, як-от у великому складі чи супермаркеті, з точкою доступу, що має кругову діаграму спрямованості (рис. 3.5). У такому разі застосування секторних антен допомагає уникнути потенційних перешкод та забезпечити необхідний рівень сигналу в радіоканалі, що, у свою чергу, гарантує високу якість зв'язку.

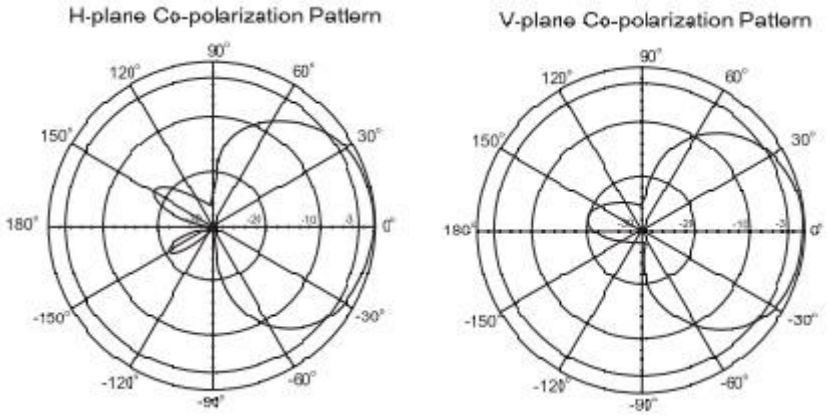

Рисунок 3.5 – Діаграма направленості антени EXT-106

ВИСНОВКИ

В рамках кваліфікаційної роботи було виконано обґрунтування для проекту «Телекомунікаційна мережа у торговельному центрі «Київ» м. Суми.

У роботі було розглянуто найпоширеніші технології передачі даних, на основі яких буде відбуватися проєктування мережі. Визначено оптимальний варіант побудови – гібридна мережа з використанням технології Ethernet у дротовій частині мережі та технології Wi-Fi стандарту 802.11ac для надання доступу до Інтернет клієнтам торгового центру та співробітникам на торгових майданчиках.

Під час вибору обладнання для реалізації проекту, перевагу було надано компанії Zyxel. Вибір обладнання ґрунтувався на таких критеріях: технічні параметри, можливості застосування, ціна та інші характеристики проектованої мережі. У розрахунковій частині роботи були проведені розрахунки корисного трафіку мережі та коефіцієнта її завантаження. Для поділу мережі на сегменти застосовувалася технологія 802.1Q VLAN.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Стандарт IEEE 802.11a, b, g, n. Бездротові мережі передачі даних Wi-Fi. [Електронний ресурс]. URL: http://www.zaomtk.com/mtk/fle/3_DOC_WIFIRus.pdf. (дата звернення 05.05.2025)

2. Стандарти Wi-Fi: IEEE 802.11ac, 802.11ax і стандарти бездротового Інтернету [Електронний ресурс]. URL: https://www.dell.com/support/contents/uk-ua/article/product-support/self-support-knowledgebase/networking-wifi-and-bluetooth/wi-fi-network-standards-overview (дата звернення 15.05.2025)

3. Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій: навч. посіб. для студ. спеціальності 121 "Інженерія програмного забезпечення", спеціалізації "Програмне забезпечення комп'ютерних та інформаційно-пошукових систем" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 225 с.

4. D-Link. Бездротове обладнання DAP-2310. [Електронний ресурс]. URL: http://www.dlink.com/ru/products/2/1480_b.html. (дата звернення 20.05.2025)

5. Zyxel. Каталог товарів: NWA 1121-NI. [Електронний ресурс]. URL: http://zyxel.com/nwa. (дата звернення 20.05.2025)

6. Zyxel. Базові положення стандарту IEEE 802.11n для Wi-Fi. Стаття 2106. [Електронний ресурс]. URL: http://zyxel.com/kb/2106. (дата звернення 22.05.2025)

7. Офіційний веб-сайт Cisco Systems. [Електронний ресурс]. URL: http://www.cisco.com/web/RU/index.html. (дата звернення 23.05.2025)

8. Сайко В. Г., Казіміренко В. Я., Літвінов Ю. М. Мережі бездротового широкосмугового доступу: навч. Посіб. Київ: ДУТ, 2015. 196 с.

9. Задерейко О.В. Комп’ютерні мережі [Електронний ресурс]: навчальний посібник / О.В. Задерейко, Н.І. Логінова, А.А. Толокнов. – Одеса, 2022. – 249 с.

10. Основи організації мереж Cisco, том 1 [Текст]: Пер. з англ. – К.: Видавничий дім «Вільямс», 2002. – 512 с.